Integrované detektory narušení

Integrated intrusion detectors

Jan Krajča

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan KRAJČA**
Osobní číslo:	**A09295**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Integrované detektory narušení**

Zásady pro vypracování:

1. **Specifikujte základní rozdělení detektorů narušení.**
2. **Vymezte a diskutujte podstatu, vlastnosti a princip činnosti integrovaných detektorů narušení.**
3. **Pojednejte o způsobech použití integrovaných detektorů narušení v prostorové ochraně.**
4. **Analyzujte a porovnejte vlastnosti vybraných integrovaných detektorů narušení.**
5. **Specifikujte trendy v oblasti integrovaných detektorů narušení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČANDÍK, Marek. Objektová bezpečnost. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. ISBN 80-731-8217-3.**
2. **ČSN EN 50131-1. Systémové požadavky. ed.2. Praha: Český normalizační institut, 2007. 40 s.**
3. **ČSN EN 50131-2-2. Detektory narušení - Pasivní infračervené detektory. Praha: Český normalizační institut, 2008. 40 s.**
4. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-807-3185-541.**
5. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. 2. vyd. Blatná: Cricetus, 2003. 351 s. ISBN 80-902-9382-4.**
6. **LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-808-7500-057.**
7. **UHLÁŘ, Jan. Technická ochrana objektů. 1. vyd. Praha: Policejní akademie České republiky, 2005. 229 s. ISBN 80-725-1189-0.**

Vedoucí bakalářské práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce pojednává o současném stavu detektorů narušení v poplachových zabezpečovacích a tísňových systémech. Cílem práce je definovat základní a nejpoužívanější detektory narušení v integraci s foto/video systémy, analyzovat na jakém principu tato zařízení pracují a zhodnotit současné představitele na trhu. Závěr práce je věnován specifikaci nejnovějších trendů v oblasti integrovaných detektorů narušení.

Klíčová slova: integrované detektory narušení, poplachový zabezpečovací a tísňový, systém, současné trendy v oblasti integrovaných detektorů narušení

ABSTRACT

Bachelor thesis deals with the current state of disruption in the intrusion and hold-up alarm system. The aim is to define the basic and most widely useddetectors disruption in the integration with photo / video systems, analyze the principle on which these devices operate and evaluate the current market leaders.The conclusion is devoted to the specification of the latest trends in integratedintrusion detector.

Keywords: integrated intrusion detectors, intrusion and hold-up alarm system, current trends of integrated intrusion detectors.

Chtěl bych poděkovat svému vedoucímu bakalářské práce doc. Ing. Luďkovi Lukášovi, CSc., za motivaci, rady a věcné připomínky, které mi poskytoval během práce. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi dostávalo během mého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

V současné době se neustále setkáváme s nárůstem všemožné kriminality. Každý den můžeme ve sdělovacích prostředcích zaslechnout zprávu o okradení důchodce ve vlastním domě, vloupání pachatelů do objektů, majetkových krádežích a podobně. Ochrana zajišťovaná státem je nedostatečná a neposkytuje občanům dostatečný pocit bezpečí, lidé stále více využívají služeb soukromých bezpečnostních složek, zprostředkovávajících různé druhy ochrany majetku. Mezi základní opatření chránící bezpečnost objektů patří technické prostředky fyzické bezpečnosti nazývané také jako technická ochrana. Pro optimální zabezpečení je často doplňována v kombinaci s režimovými opatřeními a fyzickou ochranou.

Technická ochrana není ochranou v pravém slova smyslu, ale má odradit narušitele od jeho činu, včasně zjišťovat narušení nebo napadení chráněného objektu. Mezi základní prostředky fyzické bezpečnosti patří mechanické zábranné systémy (dveře, zámky, ploty) a elektronické bezpečnostní systémy (systém kontroly vstupu, kamerové systém, poplachové zabezpečovací systémy).

Odhalení neoprávněného vniknutí nebo pokusu o vniknutí do střeženého prostoru má za úkol detektor narušení, který zjišťuje různé změny fyzikálních veličin v prostředí, způsobených činností narušitele.

Používá-li se ke zjištění stavu narušení pachatelem fyzikálních jevů, které můžou ve střeženém prostoru vzniknout i z jiných příčin, dochází pak k vyhlašování planých poplachů. Takový systém je pak z hlediska bezpečnosti nespolehlivý a nenaplňuje očekávané požadavky. Cestou pro eliminaci planých poplachů je doplnění detektorů narušení například o obrazové zjištění stavu narušení pachatelem.

V bakalářské práci se zaměřím na obecné použití detektorů narušení, dále se věnuji problémům při detekování narušení a v neposlední řadě jejich integrací s foto/video systémy.

Dále v bakalářské práci popíši specifika a princip funkce takovýchto integrovaných detektorů narušení včetně konkrétních představitelů. Závěr mé práce tvoří formulace trendů v předmětné oblasti.

I. TEORETICKÁ ČÁST

1 DETEKTORY NARUŠENÍ

Detektory narušení se v současné době řadí do skupiny prvků poplachového zabezpečovacího systému. Poplachový zabezpečovací systém je definován jako: „poplachový systém sloužící k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru“ [2].

Jde ve své podstatě o digitální elektronický systém, který v chráněném prostoru neustále sleduje předem definované fyzikální změny a při jejich výskytu vyhlašuje poplach.

Prostředky, kterými lze detekovat či zjišťovat neoprávněné vniknutí narušitele do střeženého prostoru nazýváme detektory narušení.

Detektor narušení (nazývaný také jako detektor vniknutí či detektor pohybu) je definován jako: „zařízení konstruované ke generování signálu nebo zprávy o vniknutí, jako reakci na nenormální stav detekující přítomnost nebezpečí“ [2].

Nenormální stavy detekující přítomnost nebezpečí mohou nastat z předem definovaných projevů fyzikálních změn, zejména demaskujícími projevy přítomnosti narušitele ve střeženém prostoru. Mezi takové projevy patří pohyb narušitele, změna kmitočtu odrážených akustických vln od povrchu těla narušitele nebo vyzařování infračerveného záření jeho tělem.

V případě vyvolání nenormálního stavu je detektorem vyslána poplachová zpráva, signál.

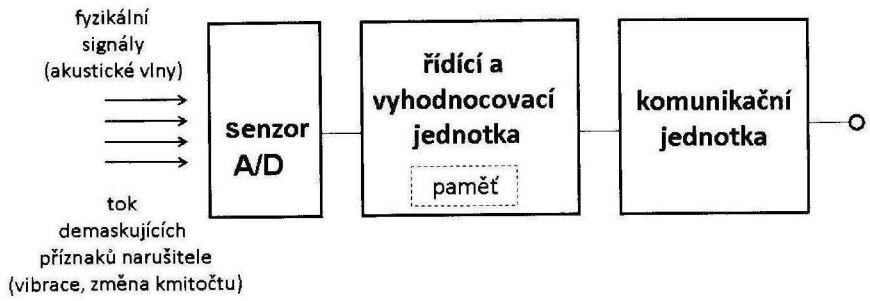
Detektor narušení monitoruje střežený prostor a v případě jeho narušení generuje poplach. Jeho úkolem je pouze informovat, že došlo k bezpečnostní kolizi, bez dalších údajů o charakteru narušení.

Obecně tvoří konstrukci detektoru narušení senzorická část, řídící a vyhodnocovací jednotka a komunikační jednotka. Úkolem senzorické části je monitorovat úroveň sledovaného fyzikálního jevu a transformovat jej v elektrický signál, který je svojí velikostí a průběhem úměrný charakteru sledovaného fyzikálního jevu. Součástí senzorické části bývá A/D převodník, který zajišťuje konverzi analogového signálu na digitální. Řídící a vyhodnocovací jednotka detektoru narušení vyhodnocuje charakter a průběh elektrického signálu, generovaného senzorickou částí. Pokud dojde ke shodě s předpokládanými signálovými projevy narušení, dojde ke generování poplachu.

Některé detektory narušení srovnávají průběh elektrického signálu, generovaného senzorickou částí, se vzorky signálu narušení, uloženými v paměti řídící a vyhodnocovací jednotky. Poplach je vyhlášen, dojde-li ke shodě obou vzorků.

Úkolem komunikační jednotky je zajistit přenos poplachu z detektorů narušení do ústředny poplachového zabezpečovacího systému po použitém přenosovém prostředí. V současnosti se k přenosu poplachu do ústředny používají jak metalických vedení, používajících jako signál elektrický proud, tak rádiových systémů, používajících elektromagnetických vln.

V některých, zejména jednodušších elektromechanických detektorech, chybí řídící a vyhodnocovací jednotka. Jedná se zejména o detektory, využívající k detekci narušení spínání spínacích kontaktů, např. magnetické kontakty [6].



Obr. 1. Blokové schéma detektoru narušení

Zdroj: Bezpečnostní technologie, systémy a management I

1.1 Základní rozdělení detektorů narušení

Detektory narušení rozdělujeme podle řady kritérií, daných principem a způsobem činností, konstrukcí, napájením, detekční charakteristikou atd.

Z pohledu energetického napájení:

- napájené
- nenapájené

Detektory napájené vyžadují ke své činnosti napájecí zdroj. Vlastní napájení může být zajištěno jak lokálním zdrojem elektrického napájení, tak dálkově po přípojném metalickém vedení z ústředny poplachového zabezpečovacího systému. Napájené detektory

obsahují elektronické obvody, zajišťující vyhodnocování monitorovaných fyzikálních jevů, kterými se prokazuje přítomnost narušitele na daném místě [6].

Napájené detektory dále dělíme, podle toho, zda vyžadují pro svou funkci vyzařování signálu do střeženého prostoru, na:

- aktivní
- pasivní

Detektory aktivní zajišťují charakteristické rysy narušení s využitím vyzařovaného signálu, elektromagnetických nebo akustický vln. Výhodou detektorů bývá jednoznačnost snímaných fyzikálních projevů narušení, např. změna kmitočtu signálu odráženého od povrchu těla narušitele. Jejich nevýhodou je naopak vyšší energetická spotřeba, nezbytnost koordinace jejich činností (elektromagnetické koexistence), plynoucí z možnosti vzájemného ovlivňování činnosti a také jejich snadná lokalizace umístění narušitelem ve střeženém prostoru.

Detektory pasivní reagují pasivně na fyzikální změny ve střeženém prostoru. Jejich výhodou je nižší energetická náročnost, obtížná zjistitelnost umístění narušitelem a snadná koexistence více detektorů ve střeženém prostoru. Nevýhodou je větší náchylnost k planým poplachům, způsobená nejednoznačností vzniku monitorovaných fyzikálních projevů [6].

Dle charakteru střežené oblasti detektory dělíme na:

- prostorové - monitorování jevů ve střežené oblasti
- směrové - monitorování jevů v definovaném směru
- bariérové - reakce na narušení bariéry (snímací detekční charakteristika)
- polohové - reakce na změnu polohy předmětu

Podle tvaru detekční (vyzařovací, snímací) charakteristiky je rozdělujeme na detektory narušení se/s:

- standardním rozsahem
- širokoúhlým rozsahem
- kruhovým rozsahem
- svislou bariérou (záclonou)

- vodorovnou bariérou (záclonou)
- dlouhým dosahem

Detektory nenapájené nevyžadují ke své činnosti zdroj napájení. Konstrukčně se jedná o velmi jednoduché systémy, pracující na principu spínání či přerušení vodiče [6].

Dle schopnosti obnovy funkce je dělíme na:

- destrukční – detektory jsou schopny pouze jednorázové funkce a po detekci narušení dojde k jejich zničení (fóliové polepy, poplachové fólie, tapety a skla)
- nedestrukční – aktivace po narušení prostřednictvím vratných změn (vibrační, magnetický kontakt, mikrospínače)

Dále detektory dělíme podle druhu ochrany, z hlediska umístění a směřování detektorů tak, aby detekovaly charakteristické rysy narušeními překonání chráněného prostoru.

Střežená zóna:

- perimetrická (obvodová)
- plášťová
- prostorová
- předmětová

Podle použitého fyzikálního signálu a principu, používaného k detekci narušení, dělíme detektory narušení na:

- elektromechanické
- elektromagnetické
- elektroakustické

1.2 Fyzikální principy a problémy detekce detektorů narušení

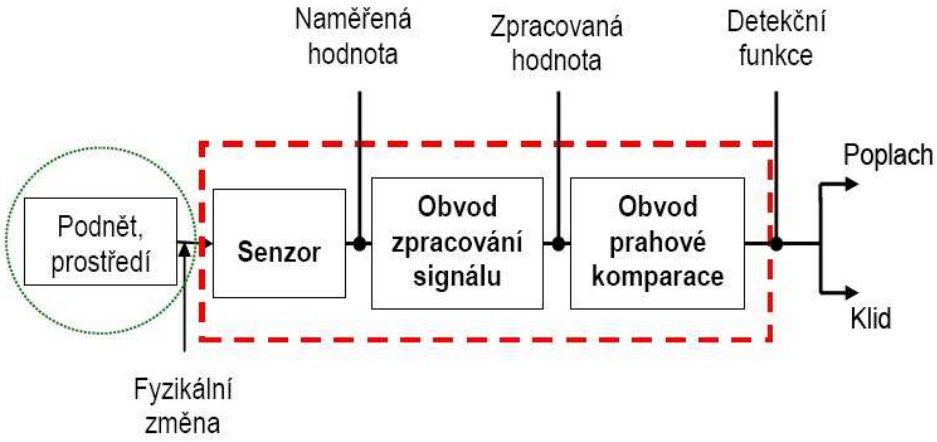
Detektory narušení plní senzorickou funkci poplachového zabezpečovacího systému, měří určitou fyzikální veličinu a převádějí ji na poplachový signál, který je přenášen dálkově do ústředny nebo na pracoviště dohledového a poplachového přijímacího centra. Schopnost detektoru narušení rozpoznat přítomnost narušitele ve střeženém prostoru je dána různými faktory. Hlavní roli sehrává fyzikální jev, který je vyvolán přítomností a pohybem

narušitele. Zejména se jedná o jeho jedinečnost, rozpoznatelnost a snadnost zachycení senzorem detektoru narušení. Používané fyzikální jevy mají mechanickou povahu, případně používají elektromagnetických a akustických vln.

Použije-li se k odhalení narušitele fyzikální jev, který může ve střeženém prostoru s velkou pravděpodobností vzniknout i z jiných příčin, dochází k vyhlašování planých poplachů. Takovýto systém je z hlediska bezpečnosti nespolehlivý a nenaplňuje očekávané požadavky [6].

1.2.1 Elektromechanický princip

Obecně lze elektromechanické detektory narušení popsat jako zařízení (prvky), reagující na mechanické (fyzikální) změny, které jsou následně převedeny na výstupní veličinu – elektrický poplachový signál [6].



Obr. 2. Obecné schéma elektromechanického detektoru narušení

Zdroj: Bezpečnostní technologie, systémy a management I

Nejčastějšími změnami mohou být:

- Sepnutí nebo rozepnutí spínače
- Přerušení spoje elektrického obvodu
- Změna elektrického parametru senzoru (odpor, kapacita, napětí, elektrický náboj)
- Změna frekvence nebo amplitudy signálu v důsledku mechanických vibrací

Mezi nejčastěji používané detektory narušení v poplachových zabezpečovacích systémech pracujících na elektromechanickém principu patří:

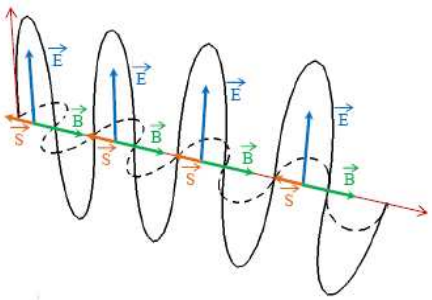
- mechanické detektory – spínače
- magnetické detektory - kontakty
- tenzometrické detektory
- kontaktní detektory destrukce skleněných ploch
- nášlapné detektory
- diferenciální tlakové hadice

Zdroje planých poplachů

- kondenzace vodních par na fóliových detektorech destrukce skleněných ploch
- citlivost na trvalá zatížení u nášlapných detektorů
- citlivost na hybnost kořenů stromů a keřů způsobených poryvy větru v korunách u diferenciálních tlakových hadic

1.2.2 Elektromagnetické záření

Úvodem lze uvést, že fyzikální podstatou většiny detektorů narušení je využívání energie záření elektromagnetického pole. Senzory detektorů narušení využívají elektromagnetického záření jako nosného média, které nese informaci o pohybu narušitele. Elektromagnetické pole můžeme popsat jako vzájemné působení elektrického a magnetického pole. Elektromagnetické záření je představováno vzájemným působením elektrického pole, které je kolmé k působení pole magnetického. Jak je z následujícího obrázku patrné, elektrické pole reprezentuje vektor elektrické indukce E a magnetické pole vektor magnetické indukce B. Oba vektory jsou kolmé na směr šíření vlny [6].



Obr. 3. Znázornění elektromagnetického pole

Zdroj: Bezpečnostní technologie, systémy a management I

Rychlost elektromagnetického vlnění je téměř totožná s rychlostí světla. Vlnovou délku elektromagnetické vlny lze vyjádřit vztahem:

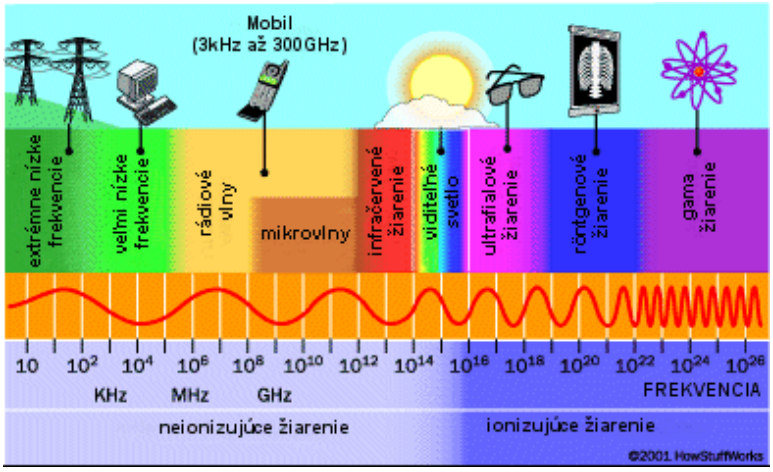
$$\lambda = c/f\,[m]$$

λ – *vlnová délka* $[m]$

c – *rychlost vlny* $[m/s]$

f – *frekvence vlnění* $[Hz]$

Elektromagnetické záření rozdělujeme pomocí vlnové délky nebo frekvence do několika oblastí. Jelikož v minulosti byly postupně objevovány jednotlivé druhy záření, byla sestavena tabulka, která určuje jejich původ vzniku. Jednotlivá záření byla pojmenována a ke každému byl přiřazen interval frekvence nebo vlnové délky [6].



Obr. 4. Elektromagnetické spektrum

Zdroj: http://hockicko.utc.sk/semestralky/prace/p37/inter3.htm

1.2.2.1 Oblast rádiových vln

Rádiové vlny představují část spektra elektromagnetického záření s frekvencemi od 10^3 – 10^{11} *Hz*. Těmto frekvencím odpovídají vlnové délky v rozsahu 10^{-1} – 10^5 *m*. Šíření rádiových vln je ovlivňováno vlnovou délkou, vertikálním složením atmosféry, tvarem zemského povrchu a překážkami na zemském povrchu. Radiové vlny se mohou šířit dvěma základními způsoby, a to podél zemského povrchu nebo ohybem kolem něho. Pokud se vlny šíří podél zemského povrchu, jde o šíření přízemní vlnou. V druhém případě se vlnění odráží od některé z ionosférických vrstev.

Princip činnosti detektorů narušení v oblasti rádiových vln je založen na změně homogenity elektromagnetického pole vytvořeného v chráněném prostoru mezi vysílací a přijímací anténou, které jsou umístěny na protějších stranách chráněného prostoru. Jakákoliv změna homogenity elektromagnetického pole, tj. narušení chráněného prostoru, způsobí odraz elektromagnetického pole (příp. změnu frekvence) vyzářeného vysílací anténou.

Na přijímací straně dojde k fázovému posuvu signálu, tzn. kmitočtu přicházejícího přímo z vysílací antény a kmitočtu odraženého od narušitele. Tento fázový posun je vyhodnocován a při překročení předem nastavené diference dojde k vyhlášení poplachu.

V současnosti se detektory narušení pracující na takovémto principu používají velmi zřídka [6] [7].

Detektory pracující v oblasti rádiových vln jsou:

- VKV detektory

Zdroje planých poplachů

- citlivost v důsledku sčítání fázových posunů
- pohyb cizých předmětů

1.2.2.2 Oblast mikrovlnného záření

Mikrovlnné záření je charakterizováno frekvencemi 10^9 – 10^{11} *Hz* a vlnovými délkami velikosti od 1 milimetru do 1 metru. Mikrovlnné záření má mnoho společného se zářením viditelným. Šíří se přímočaře, láme se a v určitých případech se může koncentrovat do jednoho bodu. K lomu a odrazu mikrovln dochází na rozhraní dvou materiálů rozdílných

dielektrických vlastností, tedy na přechodu mikrovln ze vzduchu do různých látek. O podílu odraženého a dále postupujícího mikrovlnného záření rozhoduje především rozdíl elektrických vlastností obou prostředí, ale i úhel dopadu mikrovln na plochu rozhraní. Tento typ záření se využívá například k ohřevu látek, které obsahují vodu. Při průchodu mikrovlny látkou se molekuly rozkmitávají, a v důsledku velkého tření mezi molekulami se začne prudce zvedat teplota látky.

Mikrovlny prochází objekty ze skla, z plastů, z keramiky a odrážejí se od objektů z kovu. Využití mikrovlnné záření je u elektromagnetických detektorů pohybu rozděleno do dvou různých metod:

• ***metoda Fresnelovy zóny***

Metoda Fresnelovy zóny využívá toho, že mikrovlnné záření se snadno pohltí okolními objekty nebo se od nich odrazí. Fyzikálním principem činnosti je změna energie přijímací antény mezi vysílací a přijímací parabolickou anténou. Vysílací anténa emituje mikrovlnný signál, který je registrován anténou přijímací. Přičemž Fresnelova zóna je oblast mezi oběma anténami, ve které je přenášena část mikrovlnného signálu a představuje chráněnou zónu.

Metoda Fresnelovy zóny se využívá u detektorů pohybu perimetrické ochrany. Tyto detektory nazýváme mikrovlnné zábrany a bariéry.

• ***metoda Dopplerova jevu***

Tato metoda popisuje změnu frekvence a vlnové délky přijímaného signálu oproti vyslanému signálu způsobenou nenulovou vzájemnou rychlostí vysílače a přijímače [16].

Metoda Dopplerova jevu se využívá v prostorové ochraně objektů u mikrovlnných nástěnných detektorů pohybu.

Zdroje planých poplachů

- spínání zářivkového osvětlení
- pojíždějící vozidla, výtahy
- voda protékající v plastových trubkách
- výskyt velkých kovových objektů v blízkosti detektoru

1.2.2.3 Oblast infračerveného záření

Infračervené záření je charakterizováno frekvencemi $10^{12} – 10^{14}$ *Hz* o vlnových délkách od 10 μm do 10 μm. Samotné pojmenování infračerveného záření pochází z principu ohraničení oblasti viditelného světla. Horní hranice viditelného světla je ohraničena fialovou barvou, označované z anglického názvu *violet* - *UV*. Dolní hranice viditelného světla je ohraničena barvou červenou[2], označované z anglického názvu *infra red* - *IR*. Infračervené záření se tedy nachází pod spodní hranicí viditelného záření a je pro lidské oko i řadu živočichů neviditelné. Infračervené záření má ovšem výrazné tepelné účinky. Pro člověka je infračervené záření neviditelné, protože i lidské oko vyzařuje infračervené paprsky a tím by bylo oslepeno vlastním vydávaným světlem. Člověk ale může toto záření pociťovat jako teplotní vjem. Infračervené záření vlivem absorpce v lidském těle může způsobit zahřátí tkáně a člověk tento jev pociťuje jako teplo, při větších energiích záření i jako spáleninu [16].

Tento typ záření lze získat prostřednictvím luminiscenčního, radiového nebo tepelného zdroje. U tepelných zdrojů je generování zářivého toku způsobeno rotačně-vibračními kmity atomů a molekul. Z toho tedy vyplývá, že zdrojem tepelného záření jsou všechna známá tělesa, která mají teplotu vyšší než absolutní nulu [6].

Využití infračerveného záření je u elektromagnetických detektorů rozděleno do dvou různých metod:

- ***metoda pasivního snímání***

Principem metody pasivního snímání je detekce přítomnosti infračerveného záření, které produkuje pohybující se narušitel. Pyroelektrický senzor, který se skládá z umělých materiálů, na nichž probíhá pyroelektrický jev. Obecně lze pyroelektrický jev definovat jako schopnost materiálu generovat dočasný elektrický potenciál při jeho zahřátí či ochlazení. Změnami teplot se uvnitř materiálu mírně modifikuje pozice atomů krystalové struktury a dochází k polarizaci materiálních změn.

Obr. 5. Pyroelektrický senzor

Zdroj: http://www.prlog.org/11747899-senba-d203s-pyroelectric-infrared-radial-sensor.html

Senzor ovšem dokáže registrovat pouze jednotné infračervené záření ze svého okolí. Pokud se tedy bude pachatel pohybovat před detektorem, senzor nebude schopen jeho pohyb od okolí rozlišit. Proto se využívá takzvaná segmentace střeženého prostoru. Senzor je uzpůsoben tak, aby pouze registroval tepelné záření charakteristické pro člověka – okolo 36°*C*. To zajišťuje filtr, který propouští infračervené záření pouze v rozmezí 9-10 μm. Detektor tak zachycuje pohyb těles, která mají odlišnou teplotu od okolí. Celý střežený prostor je rozdělen pomocí segmentace na aktivní a neaktivní zóny. Pokud se bude pachatel pohybovat mezi těmito zónami, na výstupu senzoru se bude generovat napěťový signál určité amplitudy a frekvence. Pro eliminaci planých poplachů se používají dvojité či dva dvojité pyroelektrické senzory. [16]

K segmentaci střeženého prostoru se používá zrcadlová optika nebo Fresnelova čočka.

Zrcadlová optika

Dříve se používala pouze kovová nedělená zrcadlová technika (odrazový systém). Průhled okénka detektoru se opatřoval mřížkou, která byla umístěna před nebo za ochrannou fólií. Postupným vývojem zrcadlové techniky došlo ke konstrukci děleného (segmentového) zrcadla, které bylo vyráběno z plastu s napařenou kovovou odraznou vrstvou. Tato zrcadla se také opatřovala černou vrstvou, která měla za úkol odfiltrovat nežádoucí složky záření a na pyroelektrický senzor se odráželo pouze IR vlnění.

Detekční charakteristika vykrytí prostoru je dána geometrií jednotlivých segmentů u zrcadla detektoru a jejich prostorovým rozložením do celku.

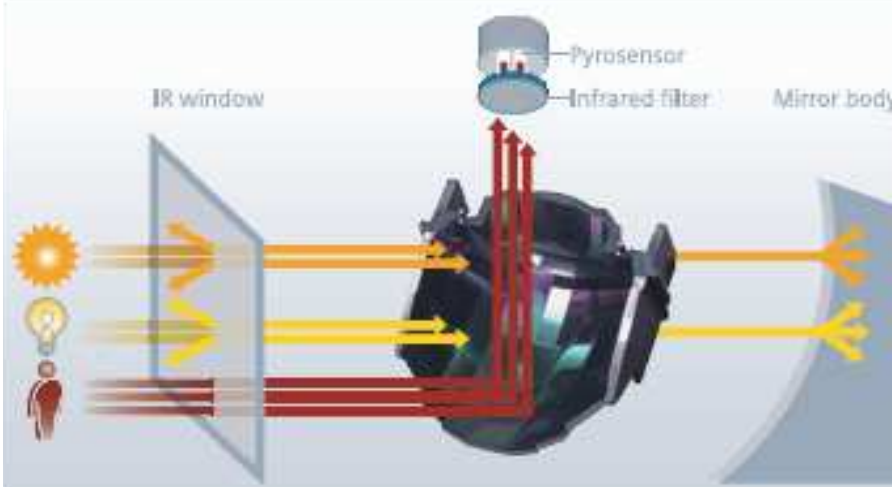
Významným trendem se stává použití černé triplexní zrcadlové optiky, kde černý podkladový materiál absorbuje rušivé zdroje bílého světla, které jsou z jiného frekvenčního

rozsahu než infračervené záření. Triplexní zrcadlová optika rozdělí hlídaný prostor až na 52 zón podobných šachovnici. Takové rozdělení umožňuje to, že i malé a velmi pomalé pohyby jsou spolehlivě detekovány a eliminuje tak další příčiny planých poplachů.

Obr. 6. Černá triplexní optika

Zdroj: http://hockicko.utc.sk/semestralky/prace/p37/inter3.htm

Až čtyřnásobný optický zoom s nastavitelnou ohniskovou vzdáleností umožňuje pokrytí pokoje jak na krátkou, tak i dlouhou vzdálenost, a to zachycením objektů v jejich skutečné velikosti v nezávislosti na vzdálenosti od detektoru [6].



Obr. 7. Filtrace bílého světla pomocí černé triplexní zrcadlové optiky

Zdroj: http://hockicko.utc.sk/semestralky/prace/p37/inter3.htm

Fresnelova čočka

Jedná o systém využívající lom paprsků. Pro její jednoduchou výrobu, nízkou cenu a hlavně snadnou změnu detekční charakteristiky detektoru (výměnou čočky) je nejvíce používána. Většinou se jedná o výlisek z umělé hmoty obsahující soustavu čoček, která zajišťuje rozdělení snímaného pole do detekčních zón.

Největší nevýhodou Fresnelových čoček je, že nemohou zajistit různé ohniskové vzdálenosti jednotlivých čoček. Z tohoto důvodu nejsou detekční zóny přesně zaostřeny na pyroelektrický senzor. To vede k poklesu amplitudy signálu ještě před jeho dalším zpracováním.

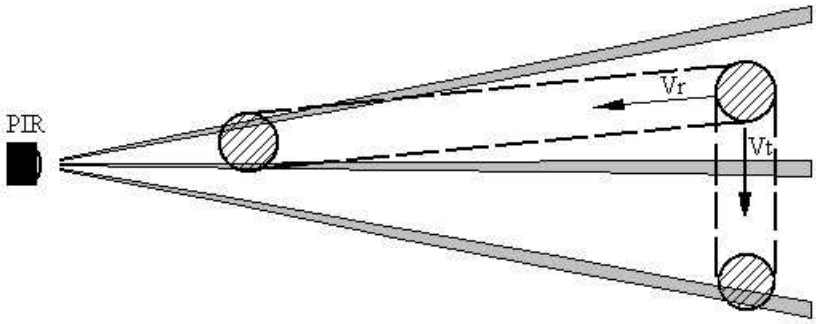
Pohyb malého živého objektu, např. myši, v bezprostřední blízkosti detektoru může vyvolat neadekvátně velkou amplitudovou odezvu, což vede v prostorách s možností pohybu hlodavců či jiných malých živočichů k vyvolání planých poplachů.

Tento problém je plně odstraněn u zrcadlové optiky, u které jsou všechny detekční zóny díky proměnné ohniskové vzdálenosti, která je zajištěna parabolickým zrcadlem, velmi přesně zaostřeny.

Optika pasivních infračervených detektorů vždy transformuje obraz zorného pole do podoby, která dalšímu elektrickému zpracování výstupnímu signálu pyroelektrickému senzoru vyhovuje nejlépe.

Pasivního metoda snímání se využívá pro prostorovou ochranu komerčně nejrozšířenějším detektorem pohybu, který je označován zkratkou *PIR* (*Passive Infra Red*).

Přímým důsledkem detekční charakteristiky je závislost citlivosti všech PIR detektorů na směru pohybu objektu. Při radiálním směru pohybu (v_r) musí stejný objekt urazit mnohem větší vzdálenost než při pohybu o tangentě (v_t), aby byl pyroelektrickým senzorem generován stejný počet impulsů. Tangenciální směr pohybu, tj. napříč detekční zónou, je směrem největší citlivosti PIR detektoru, a proto z hlediska zachycení detektorem je nejvhodnější pro předpokládaný pohyb narušitele. [7]



Obr. 7. Závislost citlivosti PIR detektoru na směru pohybu osoby

Zdroj: Technická ochrana objektů

Zdroje planých poplachů

- světelné rušení: svit slunce dovnitř místnosti, světlomety automobilů
- rychlé teplotní změny: podlahové vytápění, technické zařízení v místnosti
- zařízení místnosti: pohybující se závěsy, žaluzie
- faxovací přístroje: list termopapíru padají z faxu
- pohybem zvířat: psy, kočky, myši, ptáci apod.
- proudění vzduchu: proud teplého nebo studeného vzduchu - průvan, ventilace, topná tělesa, klimatizace

• ***metoda aktivního snímání***

Metoda aktivního snímání je podobná metodě Fresnelovy zóny jen s tím rozdílem, že místo mikrovlnného záření je využit paprsek infračerveného záření. Infračervený paprsek je na vysílači emitován polovodičovou diodou a na přijímači detekován infratranzistorem. Chráněná zóna je opět tvořena prostorem mezi vysílačem a přijímačem. Pokud infratranzistor stále přijímá infračervené záření, logický obvod vyhodnocuje stav přijímače jako klidový. Pokud mezi přijímač a vysílač vstoupí narušitel a přetne paprsek, infračervené záření na tranzistoru poklesne nebo se úplně ztratí. Tranzistor se přivře nebo zcela zavře a logický obvod na svém výstupu generuje poplachový signál.

Výhodou této metody je, že infračervený paprsek mezi vysílačem a přijímačem není pro lidské oko viditelný. Aby byl celý systém těžko překonatelný, jsou na straně přijímače i vysílače nainstalovány vysílací a přijímací diody. Infračervené paprsky pak probíhají synchronně, v impulsním kódovaném režimu s pseudonáhodným kódem. Přijímač, který

zná kód, přijme paprsek pouze od svého párového vysílače. Teprve po potvrzení přijímače vysílač vyšle paprsek nový. Tak lze zabránit nežádoucím vnějším vlivům, které by mohly přijímač negativně ovlivňovat - například sluneční záření, umělé osvětlení nebo pachatelem uměle simulovaný vysílač.

Pro lepší pokrytí plochy je používáno více paprsků, které se mohou i křížit [16].

Metodu aktivního snímání využívají detektory, jež nazýváme infračervené bariéry a závory. Slouží převážně pro perimetrickou ochranu.

Zdroje planých poplachů

- mlha
- padající sníh
- sluneční svit

1.2.2.4 Akustické vlnění

Tato metoda pracuje na bázi Dopplerova jevu. Jako detekčního média pohybu narušitele však nevyužívá mikrovlnného záření, ale ultrazvukový vln.

Zvuk obecně představuje pružné vlnění, které se šíří v pružných prostředích a periodicky se mění v prostoru a čase. Pokud naše ucho vnímá zvuk jako takový, frekvence pružného vlnění se nachází v intervalu mezi 16 *Hz* a 16 *kHz*. Jelikož vzduch má určitou pružnost a setrvačnost, mohou se v něm šířit zvukové vlny. Ty vznikají při náhlé změně hustoty vzduchu na různých místech. Rychlost šíření zvuku je závislá na teplotě a tlaku okolního vzduchu.

Ultrazvuk je zvuk, který má frekvenci větší než *16 kHz*. Jelikož vlnové délky jsou mnohem menší (řádově v milimetrech), může se ultrazvuk šířit přímočaře ve tvaru úzkých paprsků, jenž se lámou, odrážejí a soustřeďují do jednoho ohniska.

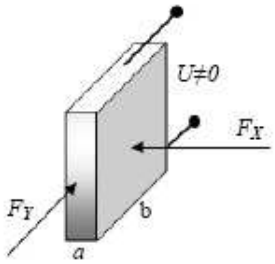
Ultrazvuk může procházet i neprůhlednými materiály. Co se týče intenzity, umělými zdroji ultrazvuku můžeme dosáhnout hodnot až $1 W/m^2$.

Ultrazvukem lze tedy do prostředí přenášet značnou energii a vytvářet jeho změnu tlaku. Podstatou metody ultrazvukových vln je Dopplerův jev, který využívá změn energie

mikrovlnného vlnění, konkrétně rozdíl mezi vysílanou a přijímanou frekvencí a to užitím vysílače a přijímače.

Vysílač emituje do chráněné zóny ultrazvukové vlny, které se odrážejí od okolních objektů zpět do přijímače. Po detekční zkoušce opět logický obvod vyhodnocuje rozdíl mezi přijatým a vyslaným kmitočtem. Objeví-li se v chráněné zóně pohybující se narušitel, dojde ke změně přijímaného signálu a na výstupu detektoru je generován poplachový signál. Detektory, které využívají metody ultrazvukových vln, nazýváme ultrazvukové detektory pohybu. Jejich základní částí jsou dva ultrazvukové senzory.

Ultrazvukový senzor se skládá z vysílače a přijímače ultrazvukových vln. Ultrazvukový vysílač přeměňuje elektrický signál na ultrazvukové vlny. Skládá se z piezoelektrického krystalu a membrány. Piezoelektrický krystal je materiál, který při přivedení polarizovaného napětí mění svůj rozměr. Naopak pokud bude piezoelektrický krystal namáhán, dojde na jeho povrchu k vytvoření polarizovaného napětí.



Obr. 8. Piezokeramický materiál

Zdroj: Bezpečnostní technologie, systémy a management I.

Přivedeme-li na ultrazvukový vysílač vysokofrekvenční střídavé napětí, bude se měnit rozměr piezokeramického krystalu. Krystal je mechanicky spojený s membránou, která tak produkuje zvukové vlny vysokých frekvencí. Senzor vysílače se skládá z multivibrátoru, ve kterém je rozmítán vysokofrekvenční signál. Tento je dále zesílen a přiveden na piezokeramický krystal.

Opačný případ bude u ultrazvukového přijímače. Bude- li ultrazvukové vlnění dopadat na plochu membrány, bude docházet vlivem jejího pohybu k deformaci piezokeramického materiálu, na jehož povrchu se bude polarizovat napětí určité velikosti [16].

Zdroje planých poplachů

- topná a teplovzdušná tělesa
- zdroje zvuku s širokým kmitočtovým spektrem
- volně zavěšené předměty (lampy, reklamní poutače)
- zvířata (hlodavci, myši)
- změny akustických vlastností chráněného prostoru (nový nábytek)

1.2.3 Shrnutí

Z výše uvedených poznatků vyplývá, že detektory narušení využívají k detekci narušitele schopnosti jeho těla, mechanického charakteru, emitovat infračervené záření charakteristické vlnové délky, schopnosti odrážet a absorbovat ultrazvuk či elektromagnetické vlny. Takovéto fyzikální projevy však mohou nastat činností i z jiných zdrojů. Detekce narušení je pak vyvolána planými poplachy, které jsou z bezpečnostního hlediska nepřijatelné.

2 INTEGROVANÉ DETEKTORY NARUŠENÍ

Výrobci zabezpečovací techniky se snaží vyvíjet výrobky s co největší odolností proti planým poplachům a zvyšovat tak stupeň zabezpečení střeženého objektu či prostoru. Jednou z možností, jak tyto požadavky realizovat, může být integrace detektorů narušení s foto či video systémem.

Kombinace plně funkčního detektoru narušení spolu s kamerou umožňuje nejen detekovat pohyb ve střeženém objektu, ale také snímat a zaznamenávat obrazovou informaci při detekci narušení. Takové detektory pak nazýváme integrované detektory narušení.

Z hlediska rozdělení poplachových zabezpečovacích systémů řadíme integrované detektory narušení do skupiny kombinovaných detektorů narušení. Označovány jsou také jako duální detektory narušení.

Duální detektor je definován jako systém detekce narušení zájmového prostoru nezávisle dvěma senzory, které pracují každý na odlišné fyzikální podstatě. Signály však mohou být společně vyhodnoceny, aby došlo k minimalizaci možného vzniku planých poplachů.

Duální detektory, které provádí střežení daného prostředí pomocí dvou odlišných způsobů, tak dokážou zpravidla eliminovat většinu obvyklého rušení z prostředí a setkávají se s rizikovými stavy pouze v případě, že dojde ke vzniku kombinace rušení, jejichž účinky mohou ovlivnit obě části duálního detektoru [17].

Integrované detektory narušení pracují na principu kombinace detekce pohybujícího se cíle (narušitele) a detekce nerušení v oblasti viditelného světla elektromagnetického záření.

Obsluha bezpečnostní agentury, či majitel zabezpečené nemovitosti, neobdrží pouze strohou informaci o detekci narušení, ale navíc má možnost se ihned přesvědčit, kdo či co, vyvolalo detekci narušení. Takovou informaci získají prostřednictvím vizuálních snímků či video sekvencí, které integrované detektory uchovávají například na zabezpečeném serveru nebo je zasílají formou MMS obrazové zprávy na mobilní telefony, případně si je ponechávají uložené na paměťové kartě.

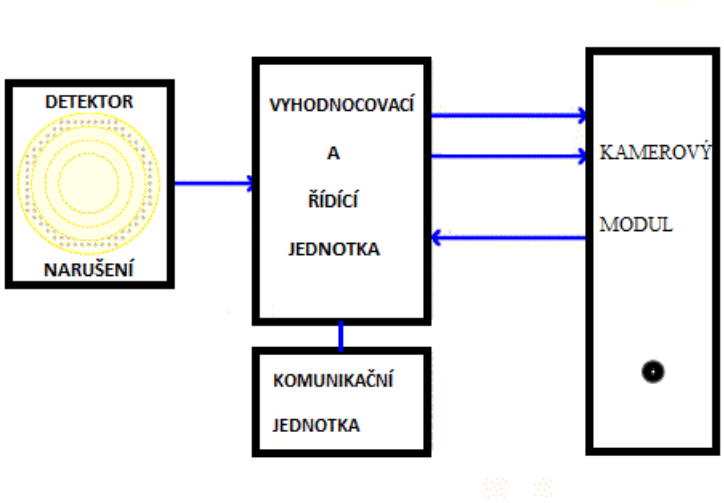
Z takto nastaveného systému zabezpečení lze již rozpoznat, zda se jednalo o planý nebo oprávněný poplach a záznam poskytnout Policii ČR pro následné stíhání možného pachatele.

Díky vizuální informaci může být okamžitě zjištěna příčina vzniku poplachu včetně průběhu narušení střeženého prostoru či objektu.

Integrované detektory narušení lze použít pro střežení objektů a prostor s vyššími nároky na zabezpečení (banky muzea, galerie, firmy), na místa s absencí fyzické ostrahy a objekty na periferii (chaty, chalupy).

Shrnutí hlavních výhod integrovaných detektorů narušení:

- vizuální potvrzení zda se jedná o oprávněný či planý poplach při detekci narušení
- zjištění příčiny, průběhu a doby trvání narušení
- zjištění přítomnosti narušitele ve střeženém prostoru či objektu
- možnost odhalení totožnosti narušitele
- kontrola pohybu narušitele po střeženém objektu či prostoru
- rychlost a dostupnost takto získaných informací



Obr. 9. Blokové schéma integrovaného detektoru narušení

Zdroj: vlastní

2.1 Konstrukce integrovaných detektorů narušení

Konstrukce detektoru musí především vycházet z funkčnosti celého detektoru. To znamená, že konstrukce detektoru musí být navržena tak, aby detektor mohl vykonávat účely, pro které byl sestrojen. Samozřejmě moderní design se podepsal i na oblasti

průmyslu komerční bezpečnosti. A tak na trhu můžeme spatřit detektory pohybu nejrůznějších tvarů, z nichž největší trend představují zaoblené hrany.

V současnosti se na trhu objevují dva typy konstrukčního provedení:

- detektor narušení + kamera
- kamera + detektor narušení

Obr. 10. Design integrovaných detektorů narušení

Zdroj: http://www.buildingtechnologies.siemens.com/bt/sp/en/security-products/intrusion_detection/Documents/FS_SP_intrusion_catalogue2009.pdf

2.1.1 Senzorická část detektoru

Senzory jsou obecně smyslovými orgány detektorů. Převádí vstupní neelektrickou veličinu na výstupní elektrickou veličinu, většinou elektrické napětí, proud nebo odpor. Přitom vstupní neelektrickou veličinou se rozumí demaskující příznaky, jimiž se prozrazuje přítomnost a pohyb narušitele na daném místě [16].

V integrovaných detektorech narušení se v současné době používají jako senzory PIR detektory pohybu.

PIR detektory mají malou spotřebu energie, vysokou spolehlivost, lze je snadno montovat a seřizovat a jejich odolnost vůči planým poplachům je značná,

Jejich další výhodou je možnost instalace více PIR detektorů do jednoho prostoru, jelikož nevyzařují pro svou funkci žádnou energii. Z důvodu aktivace PIR detektorů pouze tangenciální složkou pohybu pachatele, se doporučuje pro úplné vykrytí prostoru instalace

více detektorů a jejich vzájemné překrytí detekčních zón, bez nebezpečí vzájemného ovlivňování. [7]

Tyto detektory jsou podrobněji popsány v kapitole 1.2.2.3.

2.1.2 Kamerová část detektoru

Principiální schéma přístroje, který je schopný snímat okem viditelné světlo, tedy kamery nebo fotoaparátu, se skládá z objektivu, světlocitlivého prvku, elektronických obvodů pro zpracování informací a záznamového media.

Jako světlocitlivé prvky se používají snímací čipy CMOS a CCD.

CCD snímací čipy vytvářejí obraz vysoké kvality, zasažený jen nízkým šumem. Snímací čipy CMOS jsou oproti CCD čipům levnější, ale to je vykoupeno horšími parametry, jako je citlivost, rozlišení a spolehlivost. Energeticky více náročné jsou snímací čipy CCD.

V jednodušších aplikacích se používány méně kvalitní snímací čipy se zabudovaným objektivem, jehož ohnisková vzdálenost je konstantně dána. Pro složitější aplikace se užívají dražší snímací čipy, které se prodávají pouze jako „tělo" bez objektivu a disponují řadou funkcí jako je kompenzace protisvětla, elektronická závěrka (reguluje velikost náboje na čipu dle dopadajícího světla), řízení objektivu (závěrky) atd. Veškeré černobílé snímací čipy dnes snímají od cca 0,1 Lux (1 Lux je cca světlo svíčky), kvalitnější pak snímají například již při 0,01 Lux. Barevné snímací čipy se v dnešní době stávají cenově dostupné a k výše uvedeným funkcím zde přibývají ještě další jako je např. vyvážení bílé barvy. Barevné snímací čipy potřebují vhodnější světelné podmínky, jelikož snímají cca okolo 1 Lux. V horších světelných podmínkách lze kamerám přisvítit IR LED nebo infralampou [19].

Obr. 11. CCD a CMOS snímací čip [10]

Zdroj: http://www.azfoto.cz/informace/digital_pod_lupou/snimaci_cip

2.1.2.1 Rozlišovací schopnost snímacích čipů

Rozlišovací schopnost je hranice ostrosti snímané scény. Rozlišovací schopnost je závislá na počtu aktivních obrazových bodů snímacího čipu CCD (pixelů).

Počet pixelů se udává jako hlavní údaj o CCD či CMOS snímacím čipu. Proto rozeznáváme čipy například s 10.5 Mpix (tedy 10.5 miliónem pixelů) a podobně. Toto číslo ale samo o sobě není ten nejdůležitější údaj, sice z něj ihned vyčteme, jakým čipem je detektor osazen, ale ne kolik procent z něj dokáže využít. Například některé kamery jsou sice osazeny 8.89 Mpix CCD čipem, ale používá z něj 90% světločivných bodů - efektivní rozlišení tohoto přístroje je tedy 8 Mpix.
Oním velmi důležitým údajem je rozlišení snímku. To nám udává kolik bodů vodorovně a kolik bodů (pixelů) svisle, je schopen snímací čip rozeznat [19].

Udává se v počtu TV řádek nebo alternativně v počtech obrazových prvků (pixelech) snímacího prvku.

Rozlišení v televizních normách:

- V souvislosti s omezením normy počtu řádků a poměru stran dosáhneme maximální rozlišení, po digitalizaci obrazu pro standarty PAL 704×576 pixel a pro NTSC 704×480 pixel. To odpovídá 0.4 Mpix.

V zabezpečovací technice se používají rozlišení odvozené z těchto norem. S příchodem digitálních kamer se omezení standardy stávají bezpředmětná a začínají se používat rozlišení běžná v informačních technologiích. Jsou to hodnoty odvozené z VGA (Video Graphics Array), vyvinuté IBM pro PC. Jeho hodnota je 640x480 tj. 0.3 Mpix.

Pro jednoznačnou identifikaci osob, je nutné rozlišení alespoň 1,3 pixel na cm.

Z hlediska množství detailů ve snímané scéně je vyšší rozlišení vhodnější. Množství detailů je ve snímané scéně bude nesrovnatelné. Ze záběru pořízeného kamerou s vyšším rozlišením je mnohem snadnější, použitými algoritmy analýzy videa aplikované na vyšší rozlišení, dosáhnout přesnějších výsledků [15].

2.1.2.2 Objektiv

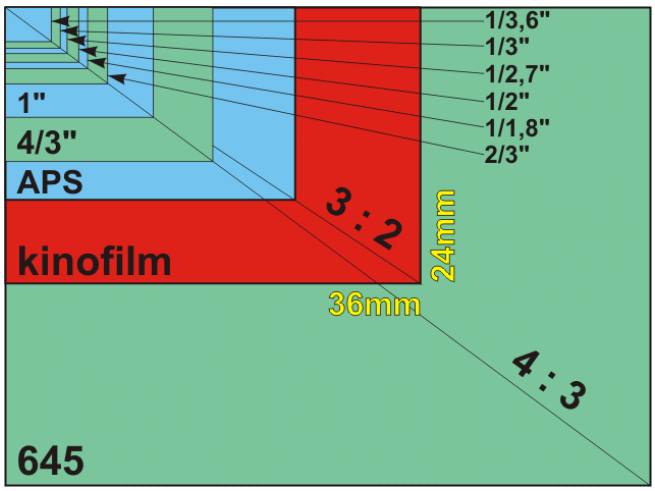
Jde prakticky o čočku nebo soustava čoček, vytvářející opticky změněný obraz, který se obvykle ještě dále zpracovává (záznamem, okulárem apod.). Používá se například ve fotoaparátu k soustředění světla na senzor nebo na film. Mezi objektivy fotoaparátu, kamery, dalekohledu, mikroskopu a dalších optických zařízení není v principu rozdíl, liší se ale svou konstrukcí.

Obr. 12. Objektiv

Zdroj: vlastní

2.1.2.3 Velikost, formát snímacích čipů a objektivů

Snímací čipy a objektivy jsou vyráběny v několika různých velikostech. Fyzicky hovoříme o délce úhlopříčky daného snímacího čipu nebo objektivu, udává se v palcích.



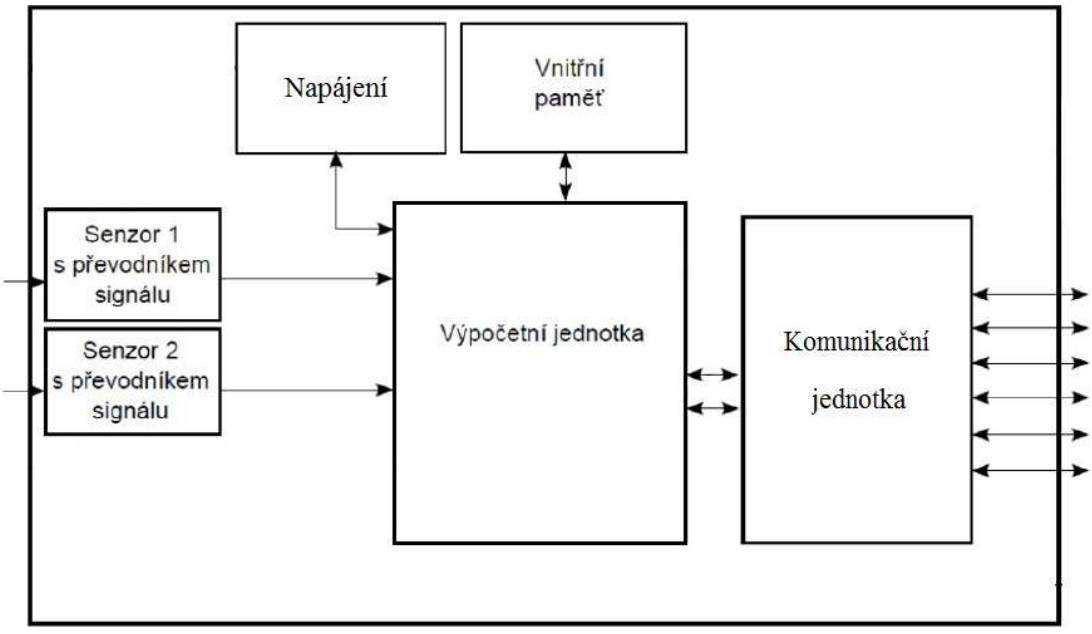
Obr. 13. Velikosti běžně používaných CCD snímacích čipů

Zdroj: vlastní

V praxi je důležité mít snímací čipy a objektiv stejného nebo většího formátu. Pokud použijete menší objektiv na větší čip (např. 1/3" objektiv na 1/2" čip), budete mít obraz orámovaný černými rohy, protože objektiv nepokrývá celou plochu snímače. Naopak když nasadíte větší objektiv na menší snímací čip (např. 1/2" objektiv na 1/4" čip) dosáhnete pravděpodobně kvalitnějšího obrazu (optika je nejpreciznější ve středu), ale zároveň bude výsledný úhel záběru menší, než při použití objektivu stejného formátu jako má snímací čip - část obrazu dopadá mimo čip.

2.1.3 Elektrická část detektoru

Účelem elektrických obvodů detektoru je vhodné zpracování výstupních signálů ze senzorů s cílem vygenerovat na výstupu poplachové signály a vizuální informaci. V aktivním stavu jsou signály z jednotlivých senzorů nejprve vyhlazeny (zbaveny šumu) a zesíleny, digitalizovány v převodnících a následně jsou předány výpočetní jednotce. Zde jsou signály porovnávány s předdefinovanými algoritmy, které jsou obvyklé pro pohyb narušitele a nakonec dochází k vyhodnocení možného poplachu, který je transformován komunikační jednotku např. do ústředny PZTS [16].



Obr. 14. Blokové schéma elektrického obvodu integrovaného detektoru narušení

Zdroj: vlastní

2.1.3.1 Senzor 1 – detektor narušení

Zpracování výstupního signálu z detektoru narušení lze rozdělit na:

Analogové zpracování signálu

Analogové detektory musí signál po přijetí nejdříve zpracovat. Při takovém zpracování putuje signál před samotnou analýzou do obvodů, které ho musí zesílit a připravit pro vstup do zpracovávacích obvodů. Signál při průchodu zesilovači a jinými nelineárními součástkami ztrácí kvalitu rozlišení a je zkreslován a také se snižuje jeho poměr Signál/šum (vlivem saturace, fázového posunu, zkreslení, výskytu šumu, ořezáním signálu apod.). Tyto vlastnosti mohou výrazně přispět k vyvolání falešného nebo planého poplachu nebo ke zkreslení důležité části informace. Přesto existují technologie, které dokážou tyto nedostatky vykompenzovat, například technologie AUTO PULSE (automatický čítač pulzů), automatická teplotní kompenzace či odolnost proti zvířatům „PET IMMUNITY“.

Digitální zpracování signálu

Při digitálním zpracování jde signál ze senzoru přes A/D převodník a po zesílení přímo do mikroprocesoru, kde je dále programově zpracován v digitální formě. Poté je podroben spektrální analýze. Přímý převod signálu do digitální podoby podstatně zlepšuje jeho rozlišení, nezkresluje průběh a zvyšuje odstup signál - šum. Oproti tradičním analogovým detektorům je signál před vlastní analýzou zatížen šumy nebo nelinearitami výrazně méně než při analogovém zpracování.

Digitální technologie radikálně snížila počet použitých součástek v detektoru, zvýšila spolehlivost a teplotní stálost, při různých frekvencích rušícího signálu detektor vykazuje rozdílnou odolnost. Tím je dosaženo zvýšení odolnosti proti planým poplachům a zároveň zvýšení procenta odhalení pohybu pachatele v hlídaném prostoru.

Efektivnost digitálních detektorů lze také zvýšit např. technologií ISG (Interlock sensor geometry) jako u detektorů analogových, nebo některou ze speciálních metod např. Digital motion detection, DIGITAL SHIELD, EEA, digitální protichůdná detekce [18].

Z hlediska vývoje poplachových zabezpečovacích tísňových systémů se pozornost trhu stále více orientuje spíše na detektory digitální. Mezi jejich hlavní výhody patří:

- integrovatelnost detektorů narušení s ostatními prvky a systémy *PZTS*

- minimalizace a integrace elektronických součástek – vlastní mikroprocesor obsahuje paměť, A/D převodník
- zozsáhlá možnost návrhu algoritmů ke zpracování výstupního signálu ze senzoru detektoru
- jednoduchá výroba – do mikroprocesoru stačí pouze nahrát odzkoušený program

Analogové detektory jejich vlastnostem konkurují jen velmi těžce.

2.1.3.2 Senzor 2 - kamerový modul

Po dopadu světla na světlocitlivý čip dochází k převedení světelného signálu na signál elektrický. Data, která čip zpracuje, dále prochází soustavou elektronických obvodů, v kterých dochází k jejich složení do požadovaného snímku.

V případě kamer vždy vzniká soustava snímků, které souhrnně vytvářejí videozáznam.

2.1.3.3 Výpočetní jednotka

Srdcem obvodů výpočetní jednotky je mikroprocesor, který zpracovává a vyhodnocuje výstupní elektrické signály ze senzorů. Samotný mikroprocesor představuje jen logický automat pro zpracování instrukcí, je nutno do něj implementovat obslužný program. Tento program představuje posloupnost instrukcí, která zajišťuje, aby mikroprocesor pracoval tak, jak požadujeme.

Zpracování, ukládání a distribuci získaných signálů či obrazových snímků ze senzorů je v dnešní době realizováno převážně digitální formou. Nasazením mikroprocesorového řízení lze vytvářet složitější a propracovanější programy, které by lépe vyhodnocovaly signály přicházející ze senzorů.

Vyhodnocování příchozích signálů je prováděno jednotlivými senzory samostatně nebo lze užít jejich kombinace dle nastavitelného algoritmu.

Mezi takové vyhodnocovací algoritmy patří tzv. „Sensor Fusion“. Jde o algoritmy analýzy obrazu v kombinaci s IR pasivní detekcí. Signály získané z obou snímacích technik jsou vyhodnocovány současně pomocí nastavitelného algoritmu. Díky této kombinaci je dostatečně bráněno vzniku planých poplachů.

Parametry detekce lze nastavit dle:

- velikosti objektu
- pozice objektu
- časového průběhu
- rychlosti
- směru pohybu objektu

Pozice objektu:

Tělesa se pohybují konečnou rychlostí. Jestliže víme, jak dlouho trvá jeden snímek, můžeme přibližně určit, kde se bude objekt v dalším snímku nacházet.

Směr pohybu:

Touto funkcí může být detektor rozlišit ve sledované zóně směr pohybu osob. Dle potřeby je možné určit směr pohybu, který vede ke spuštění poplachu.

Detektory můžeme nakonfigurovat také ke sledování směru pohybu v obou směrech. Tuto funkci lze použít např. v prostorách, kde je povolena chůze jen v jednom směru apod

Součástí výpočetní techniky je také vnitřní paměť, do které jsou ukládány pořízené snímky dle předem definovaných hodnot a parametrů [8].

2.1.3.4 Komunikační jednotka

Cílem komunikační jednotky integrovaného detektoru narušení je umožnit přenos dat, informací, poplachových zpráva a jiných sledovaných stavů do externích prvků PZTS. Hlavním úkolem komunikační jednotky je především možnost nastavování parametrů jednotlivých senzorů či detektorů a přenos poplachového signálu.

Mezi soudobé trendy patří:

- *bezdrátová komunikace*

  GSM/GPRS je paketově-přepínané spojení, což znamená, že více uživatelů sdílí stejný přenosový kanál, data se přenášejí pouze když jsou odeslána. Celková kapacita linky může být okamžitě vyhrazena těm uživatelům, kteří zrovna posílají data v kteroukoliv chvíli, což poskytuje vyšší prostupnost tam, kde uživatelé posílají nebo přijímají data periodicky. GPRS nabízí nejvyšší přenosovou rychlost 80 Kbit/s

WIFI rozhraní je rozhraní definované standardem IEEE 802.11x a bývá současně využito s rozhraním Ethernet. Jedná se tedy o technologii bezdrátového přenosu obrazu k uživateli. Výhoda spočívá ve snadné instalaci detektoru. Je nutné připojit detektoru k napájení a mít k dispozici příslušný síťový hardware podporující wifi technologii. Určitá nevýhoda spočívá v nespolehlivosti přenosu. Může docházet k rušení signálu v daném pásmu. Pásmo, které se používá pro přenos, není licencované (2,4 *GHz*). To znamená, že může být zahlcené a je možné, že bude docházet k výpadkům, proto nebude vhodné používat tuto technologii v aplikacích, kde bude potřeba zaručit bezchybný provoz. Přenosová rychlost je v řádech od 10 Mbitů/s do 100 Mbitů/s.[20]

- *komunikace po průmyslové sběrnici RS 232, RS485*

  Používá se především v průmyslovém prostředí. Standard RS485 je navržen tak, aby umožňoval vytvoření dvouvodičového poloduplexního vícebodového sériového spoje. Má stejný základ jako standard RS232, od kterého se liší především jinou definicí napěťových úrovní, nepřítomností modemových signálů, možností vytváření sítí (též sběrnice) sestávající z až 32 zařízení a možností komunikace na vzdálenost až 1200 m (proti 20 m u RS232). Výhodou rovněž je, že linku RS485 je možné vytvořit z široce rozšířeného standardu RS232 pomocí jednoduchých převodníků úrovně.

  Přenosová rychlost u krátkých spojů (do 10 m) může být až 10 Mbitů/s. Při komunikaci na vyšší vzdálenosti musí být vedení na obou stranách zakončeno zakončovacími odpory, nebo-li terminátory. Smyslem "terminátorů" je zabránit odrazům signálu od konců vedení, rovněž pomáhají zvýšit odolnost linky proti rušivým signálům. [20]

- *komunikace pomocí sítě Ethernet*

  Jedná se v současnosti o jedno z nejrozšířenějších a nejpropracovanějších rozhraní jak v komerčním sektoru, tak v průmyslové automatizaci. Rozhraním může bez problémů přenášet jak řídící, obrazové informace, tak i poplachové signály velmi vysokými rychlostmi (od 10 Mbitů/s do 1 000 Mbitů/s po kroucené dvojlince i po optickém vláknu. Další výhodou standardu Ethernet je velká škála dostupných a levných prvků pro výstavbu rozsáhlé sítě. Navíc existují převodní zařízení

standardu Ethernet na jakýkoliv jiný protokol. Fyzické připojení je pomocí síťového konektoru s označením RJ-45. Protože je celý systém síťových produktů normalizován, není problém s kompatibilitou prvků jiných výrobců.[21]

2.1.3.5 Napájení

Napájecí zdroje, které jsou součástí PZTS musí splňovat požadavky EN 50131-6 odpovídající stupni zabezpečení a třídě prostředí, dále lze napájecí zdroje rozdělit na:

- **Typ A**

  Základní napájecí zdroj. např. síťový zdroj, a náhradní napájecí zdroj dobíjený PZTS, např. akumulátor dobíjený PZTS.

- **Typ B**

  Základní napájecí zdroj a náhradní napájecí zdroj nedobíjený PZTS. Např. akumulátor nedobíjený PZTS

- **Typ C**

  Základní zdroj napájení s omezenou kapacitou, například baterie.

Napájecí zdroj musí být schopný zajišťovat energii pro PZTS za všech podmínek, včetně během dobíjení akumulátoru po dobu uvedenou tabulce na obr. 23. Napájecí zdroj může být umístěn v jednom nebo více komponentech PZTS, nebo v samostatném krytu.

Přepnutí mezi napájením ze základního zdroje a z náhradního zdroje a zpět nesmí vyvolat poplachový stav, ani jinak ovlivnit stav PZTS.

Ve všech stupních, majících jako zdroj napájení zdroj typu C jako základní napájecí zdroj, musí být tento základní napájecí zdroj schopen napájet PZTS po dobu nejméně jednoho roku za jakýchkoli provozních podmínek. Napájecí zdroj typu C musí generovat poruchový signál nebo zprávu dříve než napětí klesne pod úroveň nutnou pro normální provoz PZTS.

Typ náhradního zdroje	Stupeň 1 h	Stupeň 2 h	Stupeň 3 h	Stupeň 4 h
Maximální doba pro nabití	72	72	24	24

Obr. 15. Tabulka - náhradní napájecí zdroj – doba nabíjení [2]

Ve všech PZTS, používajících napájecí zdroje typu A a B, musí být náhradní napájecí zdroj schopen napájet PZTS v případě výpadku základního napájecího zdroje po dobu stanovenou v tabulce na obr. 24

Během intervalu specifikovaných v tabulce na obr. 24 musí být napájecí zdroj schopen poskytovat energii nutnou pro normální provoz PZTS. včetně dostatku energie pro generování veškerých povinných indikaci a hlášení vyplývajících ze zpracování dvou samostatných signálů nebo zpráv vniknutí.

Typ napájecího zdroje	Stupeň 1 h	Stupeň 2 h	Stupeň 3 h	Stupeň 4 h
Typ A	12	12	60	60
Typ B	24	24	120	120

Obr. 16. Tabulka - minimální doba napájení náhradním napájecím zdrojem [2]

Je-li v PZTS stupně 3 a 4 porucha základního napájecího zdroje hlášena do přijímacího poplachového centra nebo jiného vzdáleného centra, muže být kapacita náhradního napájecího zdroje poloviční.

Hlášení poruchy základního napájecího zdroje může být zpožděno nejvýše o 1 hodinu.

Je-li u napájecích zdrojů typu A a B použit přídavný základní napájecí zdroj s automatickým přepínáním mezi základním a přídavným napájecím zdrojem, muže být požadavek na kapacitu náhradního napájecího zdroje snížen na 4 hodiny.

Ve všech stupních PZTS musí být poskytnuta indikace, klesne-li napětí náhradního napájecího zdroje pod úroveň nutnou pro správnou funkci PZTS.

Hodnota napětí při němž je indikace poskytnuta nemá přímou souvislost s dobou, po niž musí být náhradní napájecí zdroj schopen napájet PZTS.

V PZTS, majícím napájecí zdroj typu A, musí být náhradní napájecí zdroj nabit na 80 % maximální kapacity v časech specifikovaných v tabulce na obr. 23 [2].

2.2 Provozní režimy integrovaných detektorů narušení

Z hlediska pořizování, ukládání a způsobu přenosu snímků můžeme detektory rozdělit různé provozní režimy:

- Snímky jsou ukládány do vnitřní paměti detektorů
  a) na tzv. pevné paměti
  b) na vyjímatelná paměťová média – paměťové karty
- Snímky jsou prostředky komunikační jednotky distribuovány dále např. na zabezpečený server, mobilní telefon či e-mailovou schránku.

2.3 Odolnost proti sabotáži

Detektor narušení musí být dostatečně odolný vůči projevům narušitele, vedoucím k omezení jeho funkce či jeho úplnému vyřazení z provozu. Kontrola těchto projevů bývá realizována automaticky pomocí vhodného senzoru nebo spínače.

2.3.1 Odolnost a detekce proti neoprávněnému přístupu k součástkám a nastavovacím prvkům detektoru

Všechny součástky, nastavovací prvky a přístup k montážním šroubům, které by mohly nepříznivě ovlivnit funkci detektoru, musí být umístěny uvnitř krytu detektoru. Přístup k těmto prvkům předpokládá použít předurčených nástrojů. Je-li detektor v aktivním stavu, musí otevření krytu detektoru generovat sabotážní signál nebo zprávu.

2.3.2 Detekce odejmutí z montážního úchytu

Je-li detektor oddalován z montážní plochy, musí tento stav generovat sabotážní signál nebo zprávu.

2.3.3 Odolnost nastavené orientace

Je-li detektorem násilně otáčeno, musí již při vychýlení o 5° vyvolat sabotážní signál nebo zprávu.

2.3.4 Citlivost na rušení magnetickým polem

Komunikační jednotka detektoru musí zajistit, že vlivem působení vnějšího magnetického pole není blokováno generování ani přenos žádného signálu nebo zprávy.

2.3.5 Detekce zakrytí (antimasking)

Detektor musí zpravidla být dostatečně odolný proti omezení funkce zakrytím detekční charakteristiky. Zpravidla se požaduje, aby byl sabotážní poplach generován při zakrytí přesahujícím 180 s. Signály by měly zůstat v aktivním stavu alespoň po dobu trvání maskování. Norma stanovuje rovněž časové a prostorové charakteristiky normálního lidského pohybu rychlostí 1 m/s ve vzdálenosti větší než 1m v klidové situaci, při níž nesmí být poplach generován [6].

2.4 Použití integrovaných detektorů narušení v prostorové ochraně

Oblast působení integrovaných detektorů narušení je charakteristická vysokými nároky na bezproblémovou funkci v oblasti prostorové ochrany, minimální rizikovost vyvolání planých poplachů a odolnost před rušivými vlivy. Jejich konstrukční provedení je jak pro, vnitřní, tak i vnější použití a s využitím clon lze zpravidla dosáhnout vějířového, záclonového nebo ve výjimečných případech i kruhového pokrytí. Požadovaným cílem je vždy spolehlivě vyhlásit poplach v případě, že do zájmového prostoru vstoupí narušitel v době střežení a senzory tedy slouží jako velmi rychlé a spolehlivé indikátory narušení, které jsou navíc uzpůsobeny k pořízení vizuální informace o vzniklém stavu. V případě vyhlášení poplachu tedy vzniká z dané oblasti konkrétnější zpráva o možném vzniku a průběhu narušení.

Specifické využití těchto detektorů spadá do oblasti ohraničené z jedné strany detektory pohybu PZTS a z druhé strany kamerového systému. Jedná se obvykle o místa, která vyžadují vyšší stupeň zabezpečení. Tyto detektory jsou také zvoleny při větších projektech do rizikových prostor, u kterých je předpoklad napadení zkušeným pachatelem. Kromě rizikových prostor jsou také nasazovány do míst, kde hrozí vyvolání planých poplachů a objektů bez fyzické ochrany.

II. PRAKTICKÁ ČÁST

3 ANALÝZA VLASTNOSTÍ VYBRANÝCH INTEGROVANÝCH DETEKTORŮ NARUŠENÍ

Na trhu se zabezpečovací technikou jsou v současné době k dispozici integrované detektory narušení od různých výrobců. Mezi hlavní společnosti, které na českém trhu tyto produkty nabízejí, patří:

- JABLOTRON ALARM, a.s. - JA-84P bezdrátový PIR detektor s kamerou
- Siemens, s.r.o. - IRO840T EYETEC
- EUROSAT CS, spol. s r.o. – Memo Cam Plus
- Axis – Kamera s PIR detektorem M1054

V následujících bodech budu podrobněji jednotlivé výrobky popisovat a analyzovat.

3.1 MemoCam Plus

Jedná se o PIR detektor zahrnující digitální CCD kameru s automatickým záznamem komprimovaných statických snímků nebo krátkých videosekvencí do paměťové karty. Při klidové činnosti může být neustále prováděn záznam do mezipaměti (v intervalech 4 snímky/s až 1 snímek / 5 min), což umožňuje využití záběrů pořízených před i po poplachové události. Nahrávání může být aktivováno jak vnitřním PIR detektorem, tak i vnějším „ochranným" kontaktem v případě pokusu o proniknutí do vnitřní části detektoru.

Obr. 17. MemoCam Plus

Zdroj: http://www.sourcesecurity.com/docs/fullspec/Eyetec%20brochure_en.pdf

K analýze snímků a nahrávek je nutné paměťovou kartu z detektoru vyjmout a vložit do čtečky paměťových karet připojené k PC. Výsledný záznam lze prohlížet přímo v PC po načtení paměťové karty za pomocí dodávaného programu. Nastavení parametrů MemoCam (kvalita snímků, četnost záznamu snímků, doba záznamu pří poplachu, doba odstupu poplachů, odstraňování snímků nebo záznam do zaplnění paměťové karty či nahrávání před poplachem) se provádí taktéž za pomocí paměťově karty připojené k PC a posléze zpětně vložené do MemoCamu.

Přiložené dálkové ovládání umožňuje také aktivovat či deaktivovat funkci automatického záznamu.

3.1.1 Obecné charakteristiky detektoru

Tab. 1. Tabulka parametrů MemoCam

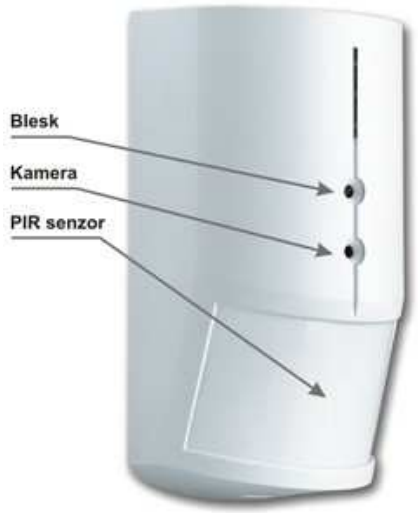
Napájení	12 V DC
Typická životnost baterie	-
Komunikační pásmo	-
Komunikační dosah	-
Část detektor narušení:	PIR
Úhel detekce	90°
Délka záběru	2-10 m
Optický systém	Fresnelova čočka
Část kamerový modul:	
Celkové rozlišení	640 x 480 bodů, černobílé
Snímací zařízení	CCD
Objektiv	Pevný kulovitý objektiv, F4.3mm
Úhel zorného pole	-
Minimální osvětlení	0.1 Lux
Formát snímku vnitřní/přenášený	JPEG na vnitřní paměťové kartě
Nastavení kvality snímku	Ano, 4 úrovně (5kB až 20kB na obrázek)
Nahrávací poměr	Od 4 snímky/sekunda do 1 snímku/5 minut
Vestavěný mikrofon	Ne
Vestavěný reproduktor	Ne
Blesk IR přisvícení, dosah	Ne
Čas předání snímku na ústřednu	-
Čas předání snímku na server	-
Ochrana proti sabotáži	Kontakt krytu

3.1.2 Využití a zhodnocení detektoru

K výhodám tohoto zařízení bych zařadil jednoduchost pořízení záznamu a poměrně malé rozměry. Snadná instalace všude tam, kde není možné použít kabeláže. Hlavní nevýhody spatřuji v nutnosti vyjmout paměťovou kartu pro získání pořízených snímků, dále pak horší rozlišení snímků a absenci blesku [14].

3.2 Bezdrátový PIR detektor JA-84P s kamerou

Tento produkt umožňuje detekovat pohyb ve střeženém prostoru včetně vizuálního potvrzení poplachu. Kamera detektoru je vybavena bleskem a infračerveným svícením pro focení v noci. Kamera je schopna pořizovat černobílé statické snímky v rozlišení 160 x 128 bodů. Je-li zaznamenám pohyb, je pořízena sekvence fotografií. Tyto fotografie jsou uloženy v interní paměti detektoru a bezdrátově přenášeny do ústředny v komprimované podobě. Odtud jsou posílány mimo objekt. Detektor se napájen baterií a komunikuje protokolem OASiS. Pro přenos snímků mezi bezdrátovým detektorem s kamerou a komunikátory JA-80Y GSM/GPRS nebo JA-80V LAN/TEL je nutné nainstalovat do ústředny modul JA-80Q.



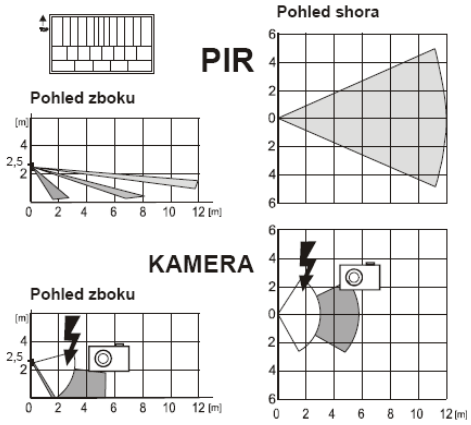
Obr. 18. Bezdrátový PIR detektor JA-84P s kamerou

Zdroj: http://www.mobotix.com/other/Products/Cameras/DualNight-M12?tab=29593#tab

Aby mohlo dojít k přenosu fotografií, musí být v ústředně odpovídající komunikátor (model JA-80Y = GSM/GPPS od verze sw. XA61006 nebo JA-80 = LAN/TEL od verze sw. XA64004) a instalován modul pro zpracování dat JA-80Q. Komunikátor umožňuje

nastavení IP adresy pro přenos fotografií. Tento server také umožňuje po přihlášení přístup k fotografiím, dále upozorní na příchod nové fotografie SMS zprávou a zpřístupní zobrazení fotografie na displeji telefonu. Další funkci, kterou server umí, je přeposílání fotografií formou e-mailu. Do jedné ústředny může být napojeno více PIR detektorů s kamerou. Pokud detektor během krátké doby vyfotí více fotek najednou, budou snímky do ústředny přeneseny ve stejném pořadí, v jakém byly detektory aktivovány. Maximální počet detektorů, které v jeden okamžik mohou přenášet snímky je osm kusů. Při vyšším počtu detektorů a současné aktivaci nemusí všechny přenosy proběhnout.

Charakteristika detekční čočky PIR nemá žádný vliv na kamerovou část detektoru. Detektor je z výroby osazen základní čočkou se zúženým záběrem 50°/12m. Prostor pokrývají 3 vějíře, které znázorňuje následující obrázek. Kamera má úhel záběru 50°, blesk přisvítí zorné pole v okruhu cca 3 metry. [15]



Obr. 19. Detekční charakteristika JA-84P

Zdroj: http://www.mobotix.com/other/Products/Cameras/DualNight-M12?tab=29593#tab

3.2.1 Obecné charakteristiky detektoru

Tab. 2. Tabulka parametrů Jablotron JA-84P

Obecné parametry:	
Napájení	2x lithiová baterie type CR123 (3.0V / 2,4Ah)
Typická životnost baterie	cca 2 roky (1 poplach měsíčně, zpožděná reakce)

Komunikační pásmo	868 MHz, protokol Oasis
Komunikační dosah	cca 300m (přímá viditelnost)
Část detektor narušení:	PIR
Úhel detekce	50°
Délka záběru	12 m
Optický systém	Fresnelova čočka
Část kamerový modul:	
Celkové rozlišení	160 x 128 bodů, černobílé
Snímací zařízení	CCD
Úhel zorného pole	-
Minimální osvětlení	0.1 Lux
Formát snímku vnitřní/přenášený	BMP/JPEG na ústřednu
Nastavení kvality snímku	
Nahrávací poměr	4 snímky za sebou po 1 sekundě
Vestavěný mikrofon	ne
Vestavěný reproduktor	ne
Blesk IR přisvícení, dosah	IR, do 3m
Čas předání snímku na ústřednu	25 sec
Čas předání snímku na server	15 s / GPRS
	2s / LAN
Ostatní parametry:	
Prostředí dle ČSN EN 50131-1	II. vnitřní všeobecné
Rozsah pracovních teplot	-10 až +40 °C
Rozměry, váha	110 x 60 x 55 mm, 140 g
Klasifikace dle	ČSN EN 50131-1, ČSN EN 50131-2-2 ČSN EN 50131-5-3 stupeň 2
Ochrana proti sabotáži	Kontakt krytu

3.2.2 Využití a zhodnocení detektoru

K výhodám tohoto zařízení bych zařadil jednoduchost záznamu, který je možný pořídit na kterémkoliv místě objektu v dosahu ústředny (cca do 300 m) bez potřeby kabeláže. Dále pak dostupnost pořízených snímků např. na zabezpečeném serveru, zasláním na e-mail či mobilní telefon. K hlavní nevýhodě bych zařadil výměny baterii (cca 2 roky) a nízkou rozlišovací schopnost kamery [17].

3.3 Eyetec IRO840T - Optický duální pohybový detektor

Konstrukce tohoto detektoru je doposud jediná na trhu a detektor tak sám vytváří novou typovou kategorii. Využití obrazového detekčního systému podpořil rozvoj techniky. Citlivost obrazového subsystému je 0,1 Lux. V případě nedostatečného osvětlení je střežení ponecháno na PIR systému a detektor je stále schopen pracovat. Nastavení perspektivy je prováděno v softwarovém rozhraní detektoru a komunikace s detektorem je na infračerveném rozhraní. Společně s novým způsobem střežení se objevily také nové nadstandardní funkce. Kromě porovnávání jednotlivých záběrů dochází k uchování 15 snímků s poplachovou událostí. Doba mezi jednotlivými snímky je nastavitelná, předem stanovená na jednu sekundu, a cílem těchto záběrů je zachytit počátek, průběh i závěr tohoto stavu. Zachycením poplachových událostí můžeme navíc identifikovat podstatu planých poplachů a minimalizovat tak riziko jejich budoucího vzniku. Mezi další vlastnosti řadíme vymezení povolených zón (nastavení povolených zón je omezeno osmi obdélníkovými výběry) a detekci a hlídání směru pohybu.

Obr. 20. Eyetec IRO480T

Zdroj: http://www.prlog.org/11747899-senba-d203s-pyroelectric-infrared-radial-sensor.html

Nastavení detektoru běžně pokrývá rozsah 90°. S dosahem 15 metrů je ideálním prostředkem k zajištění ochrany prostoru z rohu místnosti. Konstrukce ovšem umožňuje výměnu soustavy zrcadel a detektor tak lze nastavit do záclonového pokrytí, to vytváří úzký pruh, široký na svém konci jeden metr s původním dosahem. Jelikož nelze provést

změnu záběru v případě optického subsystému, je nutné v průběhu instalace využít softwarového vybavení a nastavit povolené zóny.

Porovnání softwarového rozhraní tohoto detektoru je vůči ostatním na zcela jiné úrovni. Samotný detektor má vlastní systém, umožňující volitelně nastavit nestřežené zóny v záběru scény, lze pomocí něj také určit mezičas mezi jednotlivými snímky při vyvolaném poplachu a obsahuje řadu dalších schopností. Při výsledném zhodnocení je tedy nutno podotknout, že tento hybrid dosahuje velmi vysoké úrovně zabezpečení, ale jeho nasazení je opět velmi specifické a vhodné především na místa, která nepatří mezi obvykle střežené prostory. Tyto schopnosti detektor předurčují k nasazení v galeriích, muzeích, továrních halách i vojenských objektech.

3.3.1 Obecné charakteristiky detektoru

Tab. 3. Tabulka parametrů Eyetec IRO480T

Obecné parametry:	
Napájení	12 V DC
Typická životnost baterie	-
Komunikační pásmo	IR
Komunikační dosah	do 5 m
Část detektor narušení:	PIR
Úhel detekce	90°
Délka záběru	15 m
Optický systém	černé triplexní zrcadlo
Část kamerový modul:	
Celkové rozlišení	-
Snímací zařízení	CMOS
Úhel zorného pole	-
Minimální osvětlení	0.1 Lux
Formát snímku vnitřní/přenášený	JPEG, PNG uložen ve vnitřní paměti
Nahrávací poměr	15 snímků za sebou po 1 sekundě
Vestavěný mikrofon	ne
Vestavěný reproduktor	ne
Blesk IR přisvícení, dosah	ne
Čas předání snímku na ústřednu	-
Čas předání snímku na server	-

Ostatní parametry:	
Prostředí dle ČSN EN 50131-1	II. vnitřní všeobecné
Rozsah pracovních teplot	-20 až +55 °C
Rozměry, váha	170 x 70 x 79 mm, 140 g
Klasifikace dle	50131-2 stupeň 4
Ochrana proti sabotáži	Přední a zadní kontakt krytu, AMB

3.3.2 Využití a zhodnocení detektoru

Detektor využívající PIR a obrazový detekční systém je na hranici při srovnávání systémů CCTV a duálních detektorů. Jeho konstrukce do značné míry kombinuje vlastnosti jednotlivých systémů a přenáší na sebe výhody i jistou část nevýhod. V porovnání s ostatními typy duálních detektorů je obrovskou výhodou téměř stoprocentní eliminace planých poplachů, které lze objasnit na snímcích obrazového systému. Tento systém také poskytuje nejlepší možnou metodu ochrany před zakrytím díky snímání střeženého prostoru a dokáže tak identifikovat pokusy o zakrytí jeho části i na velkou vzdálenost. [8]

3.4 IP Kamera s PIR detektorem pohybu AXIS M1054

Kamera má v sobě zabudovaný pasivní infračervený senzor (PIR) pro detekci pohybu při zhoršených světelných podmínkách, také je vybavena silnou bílou LED o výkonu 1W, která automaticky osvítí scénu, při události, která je nastavená. K tomu nabízí možnost obousměrné zvukové komunikace díky mikrofonu a reproduktoru, takže lze nejen poslouchat, co se kolem kamery děje, ale i přímo mluvit z reproduktoru nebo přes něj pouštět předem nahrané zvukové stopy.

Kamera M1031-W poskytuje několik individuálně nastavitelných streamů ve formátu H.264, ale také Motion JPEG a MPEG-4. Navíc je schopná pro každý stream podporovat plné rozlišení a plnou snímkovou frekvenci. Kompresní formát H.264 umožní optimalizovat záběry s ohledem na propustnost linky a nároky na datové úložiště.

Mezi standardní funkce patří detekce pohybu v obraze, zakrytí kamery, otočení nebo rozostření kamery či posprejování kamery. Pořízené snímky je možné zaslat na e-mail, FTP či HTTP.

Obr. 21. Kamera s PIR detektorem pohybu M1054

Zdroj: http://www.buildingtechnologies.siemens.com/bt/sp/en/security-products/intrusion_detection/Documents/FS_SP_intrusion_catalogue2009.pdf

3.4.1 Obecné charakteristiky detektoru

Tab. 4. Tabulka parametrů AXIS M1054

Obecné parametry:	
Napájení	Power over Ethernet IEEE 802.3af, 5 V DC
Typická životnost baterie	-
Komunikační pásmo	Ethernet, LAN, HTTP, FTP, SMTP
Komunikační dosah	V rámci sítě internet celosvětově
Část detektor narušení:	PIR
Úhel detekce	-
Délka záběru	6m
Optický systém	s nastavením citlivosti
Část kamerový modul:	
Celkové rozlišení	1280 x 800 pixelů, barevně
Snímací zařízení	1/4" Progressice scan RGB VGA CMOS
Objektiv	fixed focus, fixed iris, ohnisková vzdálenost: 2.9 mm
Úhel zorného pole	cca 84°
Minimální osvětlení	0 LUX
Formát snímku	

vnitřní/přenášený	JPEG/MPEG-4
Nastavení kvality snímku	ano
Nahrávací poměr	30 snímků za sekundu
Vestavěný mikrofon	ano
Vestavěný reproduktor	ano
Blesk IR přisvícení, dosah	vestavěné bílé LED přisvětlení, výkon 1W
Čas předání snímku na ústřednu	-
Čas předání snímku na server	2 s / LAN
Ostatní parametry:	
Prostředí dle ČSN EN 50131-1	-
Rozsah pracovních teplot	0°C až +40°C
Rozměry, váha	58.9 x 94.9 x 34.2 mm, 160g
Klasifikace dle	EN301489-1, EN301489-17, EN300328
Ochrana proti sabotáži	Detekce zakrytí, rozostření nebo posprejování kamery

3.4.2 Využití a zhodnocení detektoru

AXIS M1054 lze použít pro zabezpečení malých firem, restaurací, hotelů, rezidencí nebo malých objektů. Kamera disponuje standardním Eethernet síťovým připojením, lze jí zapojit do sítě internet. Výhodou je její napájení strukturovanou kabeláží. Ve své třídě nabízí velice dobrou kvalitu obrazu i při 30 snímcích za vteřinu a rozlišení 1200×800 pixel [13].

4 TRENDY V OBLASTI INTEGROVANÝCH DETEKTORŮ NARUŠENÍ

V současné době dochází díky technologickému vývoji k zavádění integrovaných detektorů narušení, které v sobě integrují detektor narušení s foto/video systémem. V oblasti ochrany osob a majetku vzniká nový způsob, kterým lze efektivněji a rychleji zjistit příčinu vzniku poplachu.

Integrované detektory narušení jsou v oblasti prostorové detekce pohybu poměrně mladou záležitostí. Svými charakteristickými vstupními vlastnostmi jsou však předurčeny k perspektivní budoucnosti.

Jelikož se jedná o mladé odvětví je potřeba tuto oblast dále zkoumat, vyvíjet a hledat možná řešení v aplikacích pro zajištění ochrany života, zdraví a majetku.

Hlavním směrem vývoje bude především:

- Miniaturizace
- Digitalizace
- Zvyšování inteligence
- Integrace

4.1 Miniaturizace

Nejen ve výrobě detektorů, ale v celém odvětví spotřební dochází k celkové miniaturizaci výrobků. Snahou výrobců zabezpečovací techniky je celkově zmenšit velikost detektoru, tak aby bylo možné jeho nasazení i do méně obvyklých míst. Miniaturní detektory nejsou z pohledu narušitele tak nápadné a rozpoznatelné jako plnohodnotná kamera či detektor pohybu.

Nevýhodou u miniaturních detektorů je, že mohou postrádat některé funkce a vlastnosti, které jsou u detektorů normální velikosti samozřejmostí (např. rozlišení, dosah).

4.2 Digitalizace

Zpracování, ukládání a distribuci získaných signálů či obrazových snímků ze senzorů je v dnešní době realizováno převážně digitální formou. Nasazením mikroprocesorového

řízení lze vytvářet složitější a propracovanější programy, které by lépe vyhodnocovaly signály přicházející ze senzorů. Vyhodnocení příchozích signálů ke generování poplachu lze provádět jednotlivými senzory samostatně nebo lze užít jejich kombinace dle nastavitelného algoritmu. Efektivní vyhodnocování signálů ze senzorů je jedna z velmi perspektivních prognóz v případě integrovaných detektorů narušení.

4.3 Zvyšování inteligence

Díky získání obrazu reálného světa z kamerového systému vznikají možnosti jeho analýzy, rozboru a následného využít ke zvýšení inteligence systému.

Mezi trendy v oblasti rozboru snímané scény paří:

- **Rozpoznávání objektů**

Výstupem po detekci objektů je rozdělení objektů ve scéně na ty co nás zajímají a na zbytek. Mezi pro nás zajímavé objekty patří objekty dostatečně velké a objekty předem určeného tvaru. K tomu jsou používány různé metody. V podstatě se jedná o nalezení co nejpočetnější množiny společných bodů a pak určit tvar této množiny.

- **Identifikace narušitele**

Identifikace člověka je klíčovým prvkem přístupových systémů kontroly vstupu. Mezi biometrické metody tohoto využívající patří: otisk prstů, podpis, geometrie tváře, vzorek duhovky, sítnice oka, geometrie ruky, geometrie prstu, tvar ucha.

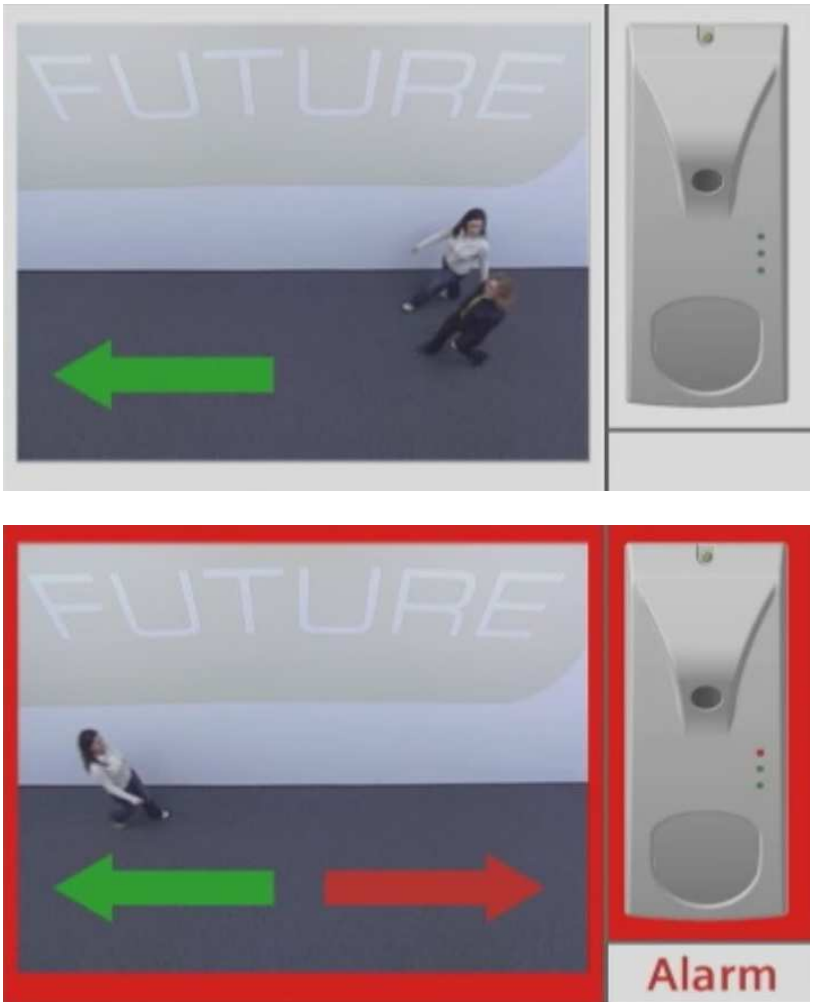
Sledovacím systémem lze zachytit, přiblížit tvář a následně vytvořit biometrickou mapu tváře z různých úhlů pohledu. Použitím vestavené databáze tváří je možné porovnávat identifikované tváře s databází a následně zobrazovat data, která jsou k těmto osobám v databázi uložena. Systém může pracovat ve dvou základních režimech.

Verifikace – porovnání jedné tváře s jednou v databázi (vhodné pro přihlašování) nebo v Identifikaci, to je porovnání jedné nebo více tváří proti tvářím uloženým v databázi. Administrátor také muže přidávat další tváře do databáze.

- **Detekce a hlídání směru pohybu**

Touto funkcí může být detektor rozlišit ve sledované zóně směr pohybu osob. Dle potřeby je možné určit směr pohybu, který vede ke spuštění poplachu.

Detektory můžeme nakonfigurovat také ke sledování směru pohybu v obou směrech. Tuto funkci lze použít např. v prostorách, kde je povolena chůze jen v jednom směru apod. [8]



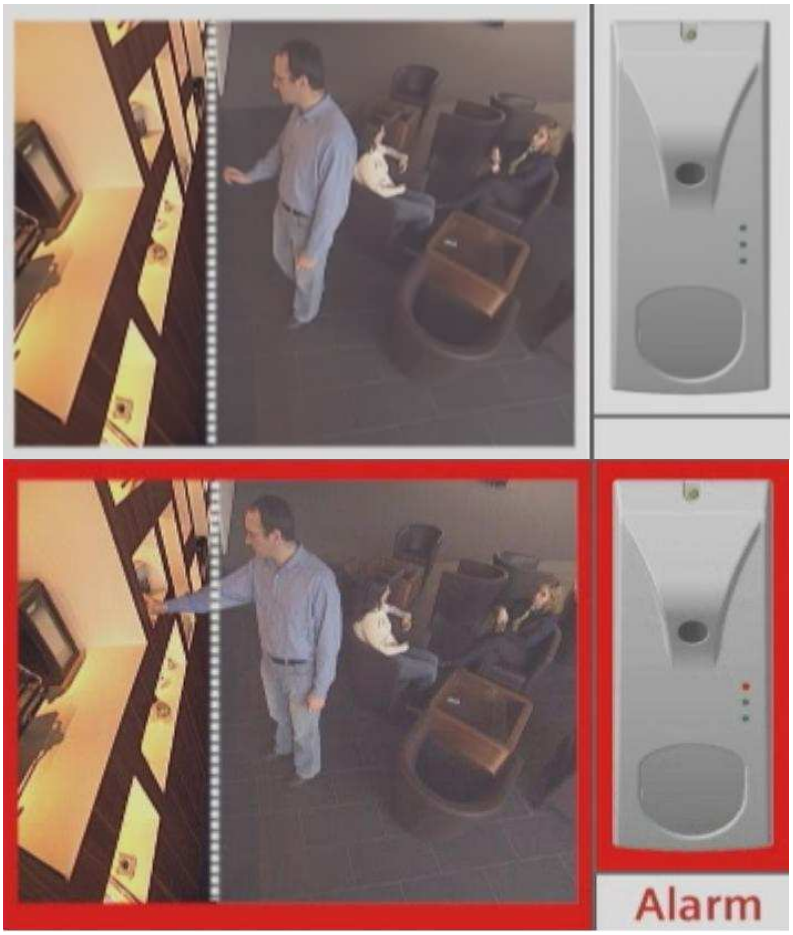
Obr. 22. Detekce chůze v protisměru

Zdroj: http://www.prlog.org/11747899-senba-d203s-pyroelectric-infrared-radial-sensor.html

- **Možnost nastavení zón ke střežení**

Jedná se o schopnost detektoru zajišťující možnost volného výběru a definování střežení jednotlivých částí z celého rozsahu záběru detektoru. To znamená, že i při aktivovaném střežení je možný pohyb ve zvolených částech prostoru a pohybující se objekty (např. stropní ventilátor, osoby) nejsou již překážkou k zastřežení.

Objekty, které se mohou nacházet v prostorech blízkým detektoru, jsou velikostně korigovány. Je u nich nastavena stejná citlivost k objektům jako ve zbylé části místnosti. [8]



Obr. 23. Volba zón střežení

Zdroj: http://www.prlog.org/11747899-senba-d203s-pyroelectric-infrared-radial-sensor.html

4.4 Integrace

Trendem v oblasti integrovaných detektorů narušení je integrace více senzorických systém do jednoho bezpečnostního prvku.

Mezi tyto systémy mohou patřit:

- Použití dvou samostatných snímacích čipů

Kdy jeden pracuje v režimu den a zaznamenává barevné snímky, druhý pak využívá černobílého snímání v nočním režimu.

Dále pak lze zavádět vícero čipů např. pro větší pokrytí střežené oblasti.

- Zavedení reproduktoru či mikrofonu

Obrazová informaci je pak doplněna o zvukový záznam, v případně reproduktoru vzniká možnost předání zvukové informace do střeženého prostoru či objektu.

Dalším trendem v oblasti integrovaných detektorů narušení je jejich integrace s jinými prvky PZTS, CCTV, EZS, MZS, ACS, SKV a inteligentními rozvody elektroinstalace v budovách.

Díky takto propojenému systému zabezpečení se může objekt tzv. aktivně bránit. To znamená rozsvítit osvětlení, spustit bezpečnostní rolety, uzamknout dveře či odpojit elektrickou energii.

Podmínkou integrace je však jednotné komunikační prostředí mezi jednotlivými prvky. Toho lze dosáhnou zavedením jednotných komunikačních protokolů nebo tzv. nástavbových integračních software.

Trendy v oblasti používaných komunikačních protokolů jsou:

- TCP/IP

  Protokol využívaný v sítích LAN a Ethernet

- ONVIF

  Jednotný komunikační protokol, který využívá 17 světových výrobců kamer.

Podle [6]“Nástavbový integrační bezpečnostní software zabezpečuje centralizované a více-uživatelské řešení pro správu PZTS“. Uživateli poskytuje nástroje pro:

- Centrální zprávu bezpečnostních systémů
- Vizualizaci a monitoring bezpečnostních systémů
- Automatizaci bezpečnostních procesů
- Analýzu a vyhodnocení bezpečnostních informací

ZÁVĚR

Bakalářská práce, zaměřená na bezpečnostní elektronické systémy, je rozdělena do dvou hlavních částí a to na teoretickou a praktickou část.

V teoretické části jsem se snažil stručně a jasně popsat základní rozdělení detektorů narušení. Dále pak jejich fyzikální podstatu, kterou jsem charakterizoval projevy mechanické povahy a využití elektromagnetických či akustických vln.

Úkolem detektoru narušení je včasné a spolehlivé zaznamenání fyzikálních projevů vzniklých z přítomnosti nebo pohybu narušitele ve střeženém prostoru. Spolehlivost detektoru narušení může být do značné míry ovlivněna skutečností, že fyzikální projevy mohou nastat i z jiných příčin než z přítomnosti a pohybu narušitele. V důsledku takových příčin dochází k vyhlašování planých poplachů, které jsou z bezpečnostního hlediska nežádoucí.

Detektory narušení zpravidla registrují pouze výskyt narušení, bez dalších údajů o jeho charakteru. Bližší informace o charakteru narušení lze získat například prostřednictvím kamerových systémů. V současné době dochází díky technologickému vývoji k zavádění integrovaných detektorů narušení, které v sobě integrují detektor narušení s foto/video systémem. V oblasti ochrany osob a majetku vzniká nový způsob, kterým lze efektivněji a rychleji zjistit příčinu vzniku poplachu.

Další kapitola teoretické části popisuje jednotlivé konstrukční a elektrické díly integrovaných detektorů narušení. Zpracování, ukládání a distribuci získaných signálů či obrazových snímků ze senzorů je v dnešní době realizováno převážně digitální formou. Nasazením mikroprocesorového řízení lze vytvářet složitější a propracovanější programy, které by lépe vyhodnocovaly signály přicházející ze senzorů. Vyhodnocení příchozích signálů ke generování poplachu lze provádět jednotlivými senzory samostatně nebo lze užít jejich kombinace dle nastavitelného algoritmu. Přenos poplachových a vizuálních zpráv je realizován komunikační jednotkou lokálně k ústředně nebo dálkově na poplachové dohledové centrum, e-mail, zabezpečený server, mobilní telefon. Uplatnění integrovaných detektorů narušení je zejména v prostorech s vysokými nároky na zabezpečení (banky muzea, galerie, firmy), na místa s absencí fyzické ostrahy a objekty na periferii (chaty, chalupy).

V praktické části jsem zanalyzoval a porovnal vlastnosti vybraných integrovaných detektorů narušení. Zejména jsem srovnal rozlišovací schopnosti snímacích čipů, způsob ukládání dat, detektory narušení, komunikační protokoly, napájení.

Trendem ve výrobě integrovaných detektorů narušení je především jejich miniaturizace, způsob vyhodnocování detekce pohybu kamerou, integrace do ostatních elektronických bezpečnostních systémů a inteligentních elektroinstalací budov, zvyšování inteligence analýzou obrazu např. identifikace osob.

ZÁVĚR V ANGLIČTINĚ

Bachelor thesis, focusing on electronic security systems, is divided into two main sections on the theoretical and practical part.

In the theoretical part, I tried to briefly describe the basic distribution of detectordistortion. Then their physical substance, which I characterized the mechanical symptoms of nature and the use of electromagnetic or acoustic waves.

The task of the detector distortion is timely and reliable record of physicalsymptoms caused by the presence or movement of an intruder in the protected area. The reliability of detector distortion can be significantly affected by the factthat the physical manifestations may happen from other causes than the presenceand movement of of an intruder. In case of such causes is the announcement offalse alarms, which are undesirable from a security perspective.

Detectors of disruption usually only registered occurrence breach, without anydetails about his character. For more information about the nature of suchdistortions can be obtained by CCTV. Currently is due to the technological developments to implement integrated distortion detectors, which integrateintrusion detector with photo / video system. As regards the protection of persons and propertyhas resulted in a method which can efficiently and quickly determine the cause of alarm.

Another chapter describes the theoretical design and electrical components of the integrated detector distortion. Processing, storage and distribution of signalsobtained from images or image sensors is nowadays mainly carried out digitally.Deployment of microprocessor control, you can create complex and sophisticatedprograms that would better evaluate the signals coming from sensors. Evaluation of the incoming signals to generate an alarm can be performed by individualsensors can be used alone or their combination adjustable according to the algorithm. Transmission of alarm messages and visual communication unit is implemented locally or remotely to the control panel for alarm monitoring center, e-mail, secure server, the mobile phone. The application of integrated intrusion detector is mainly in spaces with high security (banks museums, galleries, businesses), to the places with the absence of physical security and objects in the periphery (cottages).

In the practical part, I analyzed and compared the behavior of detectors integrateddisturbance. Especially I compared the resolving power of sensor chip, the method of data storage, intrusion detector, communication protocols, power.

The trend in production of integrated detectors is their disruption miniaturization, the method of evaluation of camera motion detection, integration with otherelectronic security systems and smart electrical installation of buildings, increaseintelligence, analysis of the image such as identification of persons.

SEZNAM POUŽITÉ LITERATURY

[1] ČANDÍK, Marek. *Objektová bezpečnost*. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. ISBN 80-731-8217-3.

[2] ČSN EN 50131-1. *Systémové požadavky*. ed.2. Praha: Český normalizační institut, 2007. 40 s.

[3] ČSN EN 50131-2-2. *Detektory narušení – Pasivní infračervené detektory*. Praha: Český normalizační institut, 2008. 40 s.

[4] KINDL, Jiří. *Projektování bezpečnostních systémů I*. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-807-3185-541.

[5] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 2. vyd. S.l.: Cricetus, 2003. 351 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-902-9382-4.

[6] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-808-7500-057.

[7] UHLÁŘ, Jan. *Technická ochrana objektů*. 1. vyd. Praha: Policejní akademie české republiky, 2005. 229 s. ISBN 80-725-1189-0.

[8] Katalog produktů a příslušenství 2009 [online]. Siemens [cit. 2012-05-17]. Dostupné z: <http://www.buildingtechnologies.siemens.com/bt/sp/en/security-products/intrusion_detection/Documents/FS_SP_intrusion_catalogue2009.pdf>.

[9] Nastavení Eyetec, nové normy [online]. Sourceserucity [cit. 2012-05-09]. Dostupné z:<http://www.sourcesecurity.com/docs/fullspec/Eyetec%20brochure_en.pdf>.

[10] Popis produktu MOMOCAM Plus [online]. Eurosat CS]. [cit. 2012-05-03]. Dostupné z: <http://www.eurosat.cz/275-memocam-plus.html>.

[11] JA-84P Bezdrátový PIR detektor s kamerou [online]. Jablotron: Manuály [cit. 2012-05-03]. Dostupné z: <http://www.jablotron.cz/upload/download/JA-84P_CZ_MHP56004.pdf >.

[12] Eytec IRO 840T optický duální pohybový detektor [online]. Siemens [cit. 2012-05-10]. Dostupné z: <http://www.siemens.cz/siemjetstorage/files/44732_Datasheet$IRO840T$CZ.pdf>.

[13] Produkty Axis [online]. Axis [cit. 2012-05-15]. Dostupné z: http://www.axis.com/products/m10_series/

[14] Produkty Eurosat [online]. Axis [cit. 2012-05-15]. Dostupné z: http://www.eurosat.cz/275-memocam-plus.html

[15] Katalog zabezpečení domů [online]. Axis [cit. 2012-05-16]. Dostupné z: http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/detektory/ja+84p+bezdratovy+pir+detektor+s+kamerou/

[16] BARÁK, Petr. Metody detekce pohybu v ochraně objektu. 2010. 98 s. Diplomová práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce Luděk Lukáš. Dostupné z: <http://dspace.k.utb.cz/bitstream/handle/10563/13139/bar%c3%a1k_2010_dp.pdf?sequence=1>.

[17] RYSNER, Jan.Duální detektory pohybu. 2006. 60 s. Bakalářská práce.Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce Luděk Lukáš. Dostupné také z: http://dspace.k.utb.cz/handle/10563/9894

[18] ODSTRČILÍK Marek. Nové typy detektorů elektrické zabezpečovací signalizace. 2006. 74 s. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce Milan Kvasnica. Dostupné také z: http://dspace.k.utb.cz/handle/10563/1786

[19] Bezpečnostní kamerové systémy CCTV [online]. Bezpečnostní kamerové systémy [cit. 2012-05-11]. Dostupné z: < http://www.kamerove-systemy-cctv.cz/ >.

[20] RS-485 [online]. Wikipedia [cit. 2012-05-09]. Dostupné z: < http://cs.wikipedia.org/wiki/RS485>.

[21] Ethernet [online]. Wikipedia [cit. 2012-05-09]. Dostupné z: <http://cs.wikipedia.org/wiki/Ethernet>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A/D	Analogově digitální převodník.
ACS	Aerospace Medicine Consultation Service.
AND	Význam třetí zkratky.
atd.	A tak dále.
AUTO PULSE	Automatický čítač pulzů
CCD	Charge Coupled Divice (nábojově vázaná struktura)
CCTV	Uzavřené střežící a dohledové systémy
CMOS	Complementary Metal–Oxide–Semiconductor, doplňující se kov-oxid-polovodič
ČR	Česká republika
DSP	Digitální signálový procesor
EZS	Elektrická zabezpečovací signalizace
GPRS	General Packet Radio Service (Obecný paketový rádiový systém, mobilní internet).
IBM	International Business Machines
IR	Infrared (infračervené záření)
ISG	Interlock sensor geometry
JPEG	Joint Photographic Experts Group - grafický rastrový formát ideální pro fotografie
LAN	Local Area Network (malá síť umožňující komunikaci mezi propojenými PC)
LED	Light-Emitting Diode (světlo-vyzařující dioda)
MJPEG	Motion Joint Picture Expert Group
MMS	Manufacturing Message Specification (Specifikace výrobních zpráv.

	Protokol pro uživatelsky orientovanou komunikaci aplikačních programů s HW výrobního procesu).
Mpix	Megapixel
MZS	Mechanické zábranné systémy
NTSC	National Television System Committee (Národní (USA) normalizační úřad pro televizní vysílání. Televizní norma)
PAL	Phase Alternating Line (Standardů kódování barevného signálu pro televizní vysílání)
PC	Osobní počítač
PIR	Passive Infra Red detektor (pasivní infračervený detektor)
PZTS	Poplachový zabezpečovací a tísňový systém
RFI/EMI	Radiofrekvenční interference/ Elektromagnetické interference
SKV	Systém kontroly vstupu
TV	Turbo Vision (Jméno SW knihovny fy Borland Int. pro programování uživatelského rozhraní aplikací).
UV	Ultrafialové záření (Ultra Violet)
VGA	Video Graphics Array
VKV	Velmi krátké vlny

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SROVNÁVACÍ TABULKA VYBRANÝCH INTEGROVANÝCH DETEKTORŮ NARUŠENÍ

	MemoCam Plus	JA-84P Bezdrátový PIR detektro s kamerou	Eyetec IRO840T Optický duální pohybový detektor	AXIS M1054 IP kamera s PIR detektorem pohybu
Obecné parametry:				
Napájení	12 V DC	2x lithiová baterie type CR123 (3.0V / 2.4Ah)	12 V DC	Power over Ethernet IEEE 802.3af, 5 V DC
Typická životnost baterie	-	cca 2 roky (1 poplach měsíčně, zpožděná reakce)	-	-
Komunikační pásmo	-	868 MHz, protokol Oasis	IR	Ethernet, LAN, HTTP, FTP, SMTP
Komunikační dosah	-	cca 300m (přímá viditelnost)	do 5 m	V rámci sítě internet celosvětově
Část detektor narušení:	PIR	PIR	PIR	PIR
Úhel detekce	90°	50°	90°	-
Délka záběru	2-10 m	12 m	15 m	6m
Optický systém	Fresnelova čočka	Fresnelova čočka	černé triplexní zrcadlo	s nastavením citlivosti
Část kamerový modul:				
Celkové rozlišení	640 x 480 pixelů, černobílé	160 x 128 pixelů, černobílé	-	1280 x 800 pixelů, barevně
Snímací zařízení	CCD	CCD	CMOS	1/4" Progressice scan RGB VGA CMOS
Objektiv	Pevný kulovitý objektiv, F4.3mm		-	fixed focus, fixed iris, ohnisková vzdálenost: 2.9 mm
Úhel zorného pole	-	-	-	cca 84°
Minimální osvětlení	0.1 Lux	0.1 Lux	0.1 Lux	0 LUX
Formát snímku vnitřní/přenášený	JPEG na vnitřní paměťové kartě	BMP/JPEG na ústředну	JPEG, PNG uložen ve vnitřní paměti	JPEG/MPEG-4
Nastavení kvality snímku	Ano, 4 úrovně (5kB až 20kB na obrázek)	-	-	ano
Nahrávací poměr	od 3 snímků/sekunda do 1 snímku/5 minut	4 snímky za sebou po 1 sekundě	15 snímků za sebou po 1 sekundě	30 snímků za sekundu
Vestavěný mikrofon	ne	ne	ne	ano
Vestavěný reproduktor	ne	ne	ne	ano
Blesk IR přísvícení, dosah	ne	IR, do 3m	IR, do 3m	vestavěné bílé LED přisvětlení, výkon 1W
Čas předání snímku na ústředну	-	25 sec	-	-
Čas předání snímku na server	-	15 s / GPRS	-	2 s / LAN
		2s / LAN		
Ostatní parametry:				
Prostředí dle ČSN EN 50131-1		II. vnitřní všeobecné	II. vnitřní všeobecné	-
Rozsah pracovních teplot		-10 až +40 °C	-20 až +55 °C	0°C až +40°C
Rozměry, váha		110 x 60 x 55 mm, 140 g	170 x 70 x 79 mm, 140 g	58.9 x 94.9 x 34.2 mm, 160g
Klasifikace dle		ČSN EN 50131-1, ČSN EN 50131-2-2 ČSN EN 50131-5-3 stupeň 2	50131-2 stupeň 4	EN301489-1, EN301489-17, EN300328
Ochrana proti sabotáži	Kontakt krytu	Kontakt krytu	Přední a zadní kontakt krytu, AMB	Detekce zakrytí, rozostření nebo posprejování kamery
Orientační cena	-	3.000,- Kč	-	8.500,- Kč